# OptiSwitch 900 Series

Carrier Ethernet Service Demarcation Devices
For
FE, GE, and 10GE Services

***Models OS904, OS906, OS910, OS910-M, OS912, and OS930***

# User Manual

## Standards Compliance

This equipment complies with the following standards: UL 60950-1:2007 CAN/CSA-C22.2 No. 60950-1-07; FCC Part 15, Class A; EMC Directive 2004/108/EC, Low Voltage Directive 73/23/EEC, RoHS Directive 2002/95/EC, NEBS/ETSI.

Class I laser products. Internal lasers comply with IEC 60 825-1:1993 + A1:1997 + A2:2001/EN60825-1:1994 + A1:1996 + A2:2001.

## FCC Notice

WARNING: This equipment has been designed to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct for the interference at the user's own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

It is suggested that the user use only shielded and grounded cables when appropriate to ensure compliance with FCC Rules.

## Disclaimer

MRV® reserves the right to make changes to any technical specifications in order to improve reliability, function, or design.

*MRV* reserves the right to modify the equipment at any time and in any way it sees fit in order to improve it.

*MRV* provides this document without any warranty of any kind, whether expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose.

The user is advised to exercise due discretion in the use of the contents of this document since the user bears sole responsibility.

## Trademarks

All trademarks are the property of their respective holders.



**Document Number:** ML49175A **Document Revision:** Rev. 09 **Release Date:** August 2010


## Contact Information

For customer support, you can:

- Contact your local MRV representative
- E-mail us at InternationalSupport@mrv.com
- Visit our MRV Web site at http://www.mrv.com


MRV Environmentally Friendly

# Contents

# Chapter 6: Ports .... 127

# Chapter 15: Extended Access Lists (ACLs)....295

# Figures

# Tables

# About this Manual

## Audience

This manual is intended for the use of the network administrator who wishes to apply, install, setup, operate, manage, and troubleshoot the OptiSwitch 900. The network administrator is expected to have working knowledge of:

- Networking
- Switches
- Routers

## Latest Revision

The latest revision of the user manual can be found at:

http://kb.mrv.co.il/Knowledge/

## Image Versions

This user manual applies to the following Master-OS™ image[1] versions of the OptiSwitch 900:

**2.1.6A** (carrier Ethernet capability)

**3.1.4** (MPLS L2 VPN capability)

(The OptiSwitch 900 *firmware* information can be viewed by invoking the CLI command **`show version`**, as described in the section *Viewing Installed Components*, page *106*.)

## Hardware Requirements

The minimum hardware requirements for running these image versions of the OptiSwitch 900 models are as follows:

For OS904, OS906, and OS912:

CPU: FER05181, 400 MHz with 32 MB Flash and 128 MB DRAM memory.

For all other OS900 devices:

CPU: MPC8245, 266 MHz with 64 MB Flash and 256 MB DRAM memory.
Device hardware version: 1 or later for OS906, OS912-AC-2, OS912-DC-2.
Device hardware version: 2 or later for OS904.
Device hardware version: 3 or later for OS910.
Device hardware version: 1 or later for OS910-M and OS930.

(The OptiSwitch 900 *hardware* information can be viewed by invoking the CLI command **`show version`**, as described in the section *Viewing Installed Components*, page *106*.)

## Features

Switching and routing features are supported in these image versions of the OptiSwitch 900. [The specific features can be viewed by invoking the CLI command **`show version`**, as described in the section *Viewing Installed Components*, page *106*.]

[1] Operative program firmware

# Related Documents

- *Release Notes for OptiSwitch 900* (produced if warranted): Contains information not found in the User Manual and/or overriding information.
- *MegaVision User Manual:* Describes how to manage the OptiSwitch 900 and other MRV SNMP-manageable products using MRV's *MegaVision Pro* ® Network Management application.
- *Outdoor Cabinets User Manual:* Describes how to install equipment in an MRV Outdoor Cabinet for protecting them in hazardous environmental conditions.

# Organization

This manual is organized into the following topics:

**Safety Requirements** – specifies the safety requirements that must be met all times.

**Chapter 1:** Overview – introduces the OS900[2]; noting its applications, architecture, key features, models, layout, and options.

**Chapter 2:** Applications – presents typical networks built with the OS900.

**Chapter 3:** Installation – shows how to mount and network connect the OS900.

**Chapter 4:** Startup, Setup, and Operation – describes how to start, set up, and run the OS900.

**Chapter 5:** CLI Management – describes how its CLI can be used to manage the OS900.

**Chapter 6:** Ports – shows how to configure the physical ports of the OS900.

**Chapter 7:** Interfaces – introduces the types of OS900 communication interface, and shows how to create, apply, manage, and obtain statistical information on them.

**Chapter 8:** Multiple-instance Spanning-Tree Protocol (MSTP) – describes how to configure the OS900 so that it can participate in the spanning-tree protocols legacy STP (IEEE 802.1**d**), Rapid STP (IEEE 802.1**w**), and Multiple-instance STP (IEEE 802.1**s**).

**Chapter 9:** ITU-T G.8032/Y.1344 Ethernet Ring Protection Switching – shows how to configure the OS900 so that it can provide Ethernet-Ring Protection switching that is compliant to *ITU-T Recommendation G.8032/Y.1344 (06/2008)*.

**Chapter 10:** Rate Limiting of Flood Packets – describes how to configure the OS900 to limit the transmission and reception data rates for certain packet types at ports of a VLAN interface.

**Chapter 11:** Provider Bridges – shows how to configure the OS900 so that IEEE 802.1Q standard VLANs can be used to interconnect remote sites of an enterprise scattered across a service provider network.

**Chapter 12:** Tag Translation/Swapping – shows how to configure the OS900 so that a packet's source VLAN tag at one UNI is swapped with that of the destination VLAN tag at another UNI (so that the packet can be received at the destination).

**Chapter 13:** IEEE 802.3ad Link Aggregation – describes how two or more ports of an OS900 can be linked in parallel to form a single logical communication channel whose bandwidth is the aggregate of the bandwidths of the individual ports.

**Chapter 14:** Quality of Service (QoS) – shows how the user can set the OS900 to give preferential treatment to each ingress and egress packet based on Layer 2 VPT or Layer 3 DSCP and, optionally, to change the VPT and DSCP values.

**Chapter 15:** Extended Access Lists (ACLs) – describes how to configure the OS900 so that it can handle ingress and egress traffic at each OS900 interface.

**Chapter 16:** Software-based Access Lists (ACLs) for Layer 2 Protocols – shows how to create and apply *software-based* Access Lists (ACLs) that handle *Layer 2 protocols*.

**Chapter 17:** SNMP Management – shows how to perform SNMP management functions on the OS900.

---

[2] OS904, OS906, OS910, OS910-M, OS912, or OS930

**Chapter 18:** Port/VLAN Mirroring – shows how to configure the OS900 so that it can replicate traffic received on one physical port or VLAN at another physical port or VLAN.

**Chapter 19:** Traffic Conditioner – describes how to configure the OS900 so that it can regulate the flow of ingress and egress traffic according to one or more packet attributes and/or conditions.

**Chapter 20:** Egress-Queue Manager (EQM) – describes how to configure the OS900 so that it can manage inbound as well as outbound traffic queues.

**Chapter 21:** IEEE 802.1ag and ITU-T Y.1731 Ethernet Service OAM – shows how to perform OAM (including fault management and performance management) of multi-domain Ethernet Services per the IEEE 802.1ag and ITU SG 13 standards.

**Chapter 22** IEEE 802.3ah OAM for Ethernet in the First Mile – shows how the OS900 can be used to perform IP-less management over an EFM link.

**Chapter 23:** Authentication, Authorization, and Accounting (AAA) – describes the RADIUS (UDP-based) and TACACS+ (TCP-based) client-server security services for restricting access to the OS900 CLI agent (via TELNET or Serial/RS-232).

**Chapter 24:** IEEE 802.1X Access Control – shows how to configure the OS900 so that it will perform authentication actions per the IEEE 802.1X standard before authorizing or rejecting connection.

**Chapter 25:** IP SLA – describes a service assurance tool that enables service providers to monitor and measure the performance of Layer 3 IP VPN routing networks.

**Chapter 26:** RFC 2544 Testing – describes the network performance analysis tool based on RFC2544.

**Chapter 27:** Scheduler – shows how to schedule execution of administrator-specified commands at times pre-set by the administrator.

**Chapter 28:** Transparent-Mode Media Cross-Connect – shows how to use the intelligent patchpanel-like functionality of the OS900.

**Chapter 29:** Firmware Viewing and Upgrading/Downloading – provides a detailed procedure for upgrading/downloading firmware to the OS900.

**Chapter 30:** Configuration Management – describes how to view, select, delete, or save a configuration, restore an erased configuration or the factory default configuration, and how to upload and download a configuration using FTP.

**Chapter 31:** Dynamic Host Configuration Protocol (DHCP) – describes how the OS900 can be configured to provide addresses to hosts on its network automatically and for a pre-specified time duration.

**Chapter 32:** BOOTstrap Protocol (BOOTP) – describes how the OS900 can be set to operate in client mode with BOOTP in order to get its IP address and/or configuration file from a DHCP server.

**Chapter 33:** Network Time Protocol (NTP) and Timezone – shows how to use the Internet standard protocol for synchronizing clocks of network devices.

**Chapter 34:** Network Address Translation (NAT) – shows how to set the OS900 so that it automatically replaces an IP address of a packet with another IP address when the packet crosses a specific network interface (port) of the OS900.

**Chapter 35:** IGMP IP Multicast – shows how to direct selective IP multicast traffic (data, voice, video, etc.) to ports belonging to a particular IP Multicast group.

**Chapter 36:** Static and Dynamic Routing – shows how static and dynamic routes can be configured on the OS900.

**Chapter 37:** WDM Module – shows how to apply and install the WDM module.

**Chapter 38:** E1/T1 CES Module – shows how to apply, install, and configure the E1/T1 module.

**Chapter 39:** STM-1/OC3 CES Module – shows how to apply, install, and configure the STM-1/OC3 CES module (EM9-CES-OC3).

**Chapter 40:** DSL Setup and Monitoring– shows how to configure the OS904-DSL4 model's Single-pair High-speed Digital Subscriber Line (SHDSL) transceiver.

**Chapter 41:** MultiProtocol Label Switching (MPLS) – shows how to utilize the technology that uses labels to direct traffic (e.g., Ethernet packets) to their destination.

**Chapter 42:** Provision – shows how to provision Layer 2 Ethernet services and to control traffic flows in services in accordance with the Metro Ethernet Forum (MEF) specifications..

**Appendix A:** Utilities – describes and shows how to use the various network utilities of the OS900.

**Appendix B:** Cable Wiring – shows the wiring for the null-modem RS-232, Ethernet straight, and Ethernet cross cables.

**Appendix C:** Cleaning Optical Connectors – describes a recommended procedure for cleaning optical connectors on the OS900.

**Appendix D:** Troubleshooting – is a guide for troubleshooting the OS900 on the operative level.

**Appendix E:** Packet Processing Stages – illustrates the processing stages through which packets pass in the OS900 from entry to exit.

**Appendix F:** Product Specification – provides the general specifications of the OS900.

**Appendix G:** Release Notes for Firmware Version 2.1.6A and 3.1.4 – contains new and/or overriding information relative to the previous version.

# Typographical Conventions

The typographical conventions used in this document are as follows:

| Convention | Explanation |
|---|---|
| **`Courier Bold`** | This typeface represents information provided *to* the OS900. |
| `Courier Plain` | This typeface represents information provided *by* the OS900. |
| *Italics* | This typeface is used for emphasis. |
| Enter | This format represents the key name on the keyboard/keypad. |
|  | This icon represents important information. |
|  | This icon represents risk of personal injury, system damage, or data loss. |

# Acronyms

| | |
|---|---|
| **AAA** | **A**uthentication, **A**uthorization, and **A**ccounting |
| **ACL** | **AC**cess **L**ist (service) |
| **ARP** | **A**ddress **R**esolution **P**rotocol (For getting MAC address) |
| **AWG** | **A**merican **W**ire **G**age |
| **BER** | **B**it-**E**rror **R**ate |
| **BOOTP** | **BOOT**strap **P**rotocol |
| **BPDU** | **B**ridge **P**rotocol **D**ata **U**nit |
| **BRAS** | **B**roadband **R**emote **A**ccess **S**erver |
| **BSD** | **B**erkley **S**oftware **D**istribution |
| **CBS** | **C**ommitted **B**urst **S**ize |
| **CC** | **C**ontinuity **C**heck |
| **CCM** | **C**ontinuity **C**heck **M**essages |
| **CDP** | **C**isco **D**iscovery **P**rotocol |
| **CE** | **C**ustomer **E**dge |

| | |
|---|---|
| **CES** | **C**ircuit **E**mulation **S**ervice |
| **CFM** | **C**onnectivity **F**ault **M**anagement |
| **CIDR** | **C**lassless **I**nter-**D**omain **R**outing |
| **CIR** | **C**ommitted **I**nformation **R**ate |
| **CIST** | **C**ommon and **I**nternal **S**panning **T**ree |
| **CL** | **C**onformance **L**evel |
| **CLI** | **C**ommand **L**ine **I**nterpreter (**I**nterface) |
| **CoS** | **C**lass **o**f **S**ervice |
| **CO** | **C**entral **O**ffice |
| **CPE** | **C**ustomer **P**remises **E**quipment |
| **CRC** | **C**yclic **R**edundancy **C**heck |
| **CR-LDP** | **C**onstrained **R**outing **LDP** |
| **CSPF** | **C**onstrained **S**hortest **P**ath **F**irst |
| **CTS** | **C**lear **T**o **S**end |
| **CWDM** | **C**oarse **W**avelength-**D**ivision **M**ultiplexing |
| **dB** | **d**eci**B**el |
| **DCD** | **D**ata **C**arrier **D**etect |
| **DES** | **D**ata **E**ncryption **S**tandard (code/algorithm) |
| **DHCP** | **D**ynamic **H**ost **C**onfiguration **P**rotocol |
| **DiffServ** | **Diff**erentiated **Serv**ices |
| **DNS** | **D**omain **N**ame **S**erver/**S**ystem |
| **DoS** | **D**enial **o**f **S**ervice |
| **DSCP** | **D**ifferentiated **S**ervices **C**ode **P**oint |
| **DSR** | **D**ata **S**et **R**eady |
| **DTE** | **D**ata **T**erminal **E**quipment |
| **DTR** | **D**ata **T**erminal **R**eady |
| **DWDM** | **D**ense **W**avelength-**D**ivision **M**ultiplexing |
| **EBS** | **E**xcess **B**urst **S**ize |
| **EFM** | **E**thernet in the **F**irst **M**ile |
| **EIA** | **E**lectronic **I**ndustries **A**lliance |
| **EPL** | **E**thernet **P**rivate **L**ine |
| **ETSI** | **E**uropean **T**elecommunications **S**tandards **I**nstitute |
| **FEC** | **F**orwarding **E**quivalence **C**lass or **F**ast **E**thernet **C**hannel |
| **FIB** | **F**orwarding **I**nformation **B**ase |
| **FLR** | **F**rame **L**oss **R**atio |
| **FPGA** | **F**ield-**P**rogrammable **G**ate **A**rray |
| **FTN** | **F**EC **T**o **N**HLFE |
| **FTP** | **F**ile **T**ransfer **P**rotocol |
| **FTTX** | **F**iber **T**o **T**he **X** (Home/Business/etc.) |
| **GMT** | **G**reenwich **M**ean **T**ime |
| **GPS** | **G**lobal **P**ositioning **S**ystem/**S**atellite |
| **ICMP** | **I**nternet **C**ontrol **M**essage **P**rotocol |
| **IEEE** | **I**nstitute of **E**lectrical and **E**lectronic **E**ngineers |
| **IETF** | **I**nternet **E**ngineering **T**ask **F**orce |
| **IGMP** | **I**nternet **G**roup **M**anagement **P**rotocol |
| **ILM** | **I**ncoming **L**abel **M**ap |

| | |
|---|---|
| **IP** | **I**nternet **P**rotocol |
| **ISDN** | **I**ntegrated **S**ervices **D**igital **N**etwork |
| **ISP** | **I**nternet **S**ervice **P**rovider |
| **ITU** | **I**nternational **T**elecommunications **U**nion |
| **LACP** | **L**ink **A**ggregation **C**ontrol **P**rotocol |
| **LAG** | **L**ink **AG**gregation |
| **LAN** | **L**ocal **A**rea **N**etwork |
| **LBM** | **L**oopback **M**essage |
| **LBR** | **L**oop**B**ack **R**eply |
| **LDP** | **L**abel **D**istribution **P**rotocol |
| **LER** | **L**abel **E**dge **R**outer |
| **LIN** | **L**ink **I**ntegrity **N**otificationF |
| **LLC** | **L**ogical **L**ink **C**ontrol |
| **LMR** | **L**oss **M**easurement **R**eply |
| **LOC** | **L**oss **O**f **C**ontinuity |
| **LOS** | **L**oss **O**f **S**ignal |
| **LRM** | **L**oopback **R**eply **M**essage |
| **LSA** | **L**ink-**S**tate **A**dvertisement |
| **LSP** | **L**abel **S**witch **P**ath |
| **LSR** | **L**abel **S**witch **R**outer |
| **LTM** | **L**inktrace **M**essage |
| **LTR** | **L**ink **T**race **R**eply |
| **MA** | **M**aintenance **A**ssociation |
| **MAC** | **M**edium **A**ccess **C**ontrol |
| **MAID** | **M**aintenance **A**ssociation **ID**entifier |
| **MAN** | **M**etropolitan **A**rea **N**etwork |
| **MD** | **M**aintenance **D**omain level |
| **MD5** | **M**essage **D**igest **5** (code/algorithm) |
| **MDI** | **M**edia **D**ependent **I**nterface<br>Pinout: 1 → Tx+, 2 → Tx-, 3 → Rx+, 6 → Rx-.<br>Connected to DTE with a cross-wired cable. |
| **MDIX** | **M**edia **D**ependent **I**nterface **X** (with cross-wiring)<br>Pinout: 1 → Rx+, 2 → Rx-, 3 → Tx+, 6 → Tx-.<br>Connected to DCE with a cross-wired cable. |
| **MDN** | **M**aintenance **D**omain **N**ame |
| **ME** | **M**aintenance **E**ntity - service |
| **MEF** | **M**etro **E**thernet **F**orum |
| **MEP** | **M**aintenance association **E**nd **P**oint |
| **MIB** | **M**anagement **I**nformation **B**ase |
| **MSTI** | **M**ultiple **S**panning-**T**ree **I**nstance |
| **MTU** | **M**ulti-**T**enant **U**nit or **M**aximum **T**ransmission **U**nit |
| **NAS** | **N**etwork **A**ccess **S**erver |
| **NAT** | **N**etwork **A**ddress **T**ranslation |
| **NEBS** | **N**etwork **E**quipment **B**uilding **S**ystem |
| **NGN** | **N**ext-**G**eneratio**N** |
| **NHLFE** | **N**ext-**H**op **L**abel **F**orwarding **E**ntry |
| **NMS** | **N**etwork **M**anagement **S**tation |

| | |
|---|---|
| **NNI** | **N**etwork-**N**etwork **I**nterfaces |
| **NOC** | **N**etwork **O**peration **C**enter |
| **NTP** | **N**etwork **T**ime **P**rotocol |
| **OADM** | **O**ptical **A**dd-**D**rop **M**ultiplexer |
| **OAM** | **O**perations, **A**dministration, and **M**aintenance<br>(Tools/utilities for installing, monitoring, and troubleshooting a network.) |
| **OC-3** | **O**ptical **C**arrier level-**3** |
| **OESD** | **O**ptical **E**thernet **S**ingle-service **D**emarcation-unit |
| **OID** | **O**bject **ID**entifier |
| **OSS** | **O**peration **S**upport **S**ystems |
| **PAF** | **PME A**ggregation **F**unction |
| **PBS** | **P**eak **B**urst **S**ize |
| **PCP** | **P**riority **C**ode **P**oint |
| **PDH** | **P**lesiosynchronous **D**igital **H**ierarchy |
| **PDU** | **P**rotocol **D**ata **U**nit |
| **PE** | **P**rovider **E**dge |
| **PHB** | **P**er-**H**op **B**ehavior |
| **PIM-SM** | **P**rotocol **I**ndependent **M**ulticast **S**parse-**M**ode |
| **PING** | **P**acket **I**nter-**N**etwork **G**roper |
| **PIR** | **P**eak **I**nformation **R**ate |
| **PME** | **P**hysical **M**edium **E**ntity |
| **PMM** | **P**erformance **M**anagement **M**essage |
| **PMR** | **P**erformance **M**anagement **R**eply |
| **PoP** | **P**oint-**o**f-**P**resence |
| **PSN** | **P**acket-**S**witching **N**etwork |
| **QoS** | **Q**uality **o**f **S**ervice |
| **RADIUS** | **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice |
| **RDI** | **R**emote **D**efect **I**ndication |
| **RED** | **R**andom **E**arly **D**iscard |
| **RIP** | **R**outing **I**nformation **P**rotocol |
| **RLB** | **R**emote **L**oop**B**ack |
| **RMON** | **R**emote **MON**itoring |
| **RoI** | **R**eturns **o**n **I**nvestment |
| **RSVP-TE** | **R**esource Re**S**er**V**ation **P**rotocol – **T**raffic **E**ngineering |
| **RTR** | **R**esponse **T**ime **R**eporter |
| **RTS** | **R**equest **T**o **S**end |
| **RU** | **R**ack **U**nit |
| **RxD** | **R**eceive **D**ata |
| **SCADA** | **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition |
| **SCP** | **S**ecure **C**opy **P**rotocol |
| **SDH** | **S**ynchronous **D**igital **H**ierarchy |
| **SFP** | **S**mall **F**orm-factor **P**luggable |
| **SL** | (DiffServ) **S**ervice **L**evel |
| **SLA** | **S**ervice **L**evel **A**greement |
| **SMB** | **S**ub-**M**iniature **B**-type |
| **SNMP** | **S**imple **N**etwork-**M**anagement **P**rotocol |
| **SONET** | **S**ynchronous **O**ptical **NET**work |

| | |
|---|---|
| **SSH** | **S**ecure **SH**ell |
| **SST** | **S**ingle **S**panning **T**ree |
| **STM-1** | **S**ynchronous **T**ransport **M**odule level-**1** |
| **TACACS** | **T**erminal **A**ccess **C**ontroller **A**ccess-**C**ontrol **S**ystem |
| **TC** | **T**raffic **C**onditioner |
| **TCO** | **T**otal **C**ost of **O**peration |
| **TCP** | **T**ransmission **C**ontrol **P**rotocol |
| **TDM** | **T**ime-**D**ivision **M**ultiplexing/**M**ultiplexer |
| **TDR** | **T**ime-**D**omain **R**eflectometry |
| **TELNET** | (dial-up) **TEL**ephone **NET**work (connection protocol) |
| **TFTP** | **T**rivial-**F**ile **T**ransfer **P**rotocol |
| **TLS** | **T**ransport **L**ayer **S**ecurity |
| **TLV** | **T**ime, **L**ength, **V**alue |
| **ToS** | **T**ype **o**f **S**ervice |
| **TTL** | **T**ime-**T**o-**L**ive |
| **TxD** | **T**ransmit **D**ata |
| **UDP** | **U**ser **D**atagram **P**rotocol |
| **UNI** | **U**ser-**N**etwork **I**nterface |
| **UPS** | **U**ninterruptible **P**ower **S**upply |
| **URL** | **U**niversal **R**esource **L**ocation |
| **UTC** | **C**oordinated **U**niversal **T**ime |
| **VACM** | **V**iew-based **A**ccess **C**ontrol **M**odel |
| **VC** | **V**irtual **C**ircuit |
| **VCD** | **V**irtual **C**able **D**iagnostics |
| **VID** | **V**LAN **ID** |
| **VLAN** | **V**irtual **LAN** |
| **VPLS** | **V**irtual **P**rivate **L**AN **S**ervice |
| **VPN** | **V**irtual **P**rivate **N**etwork |
| **VPT** | **V**LAN **P**riority **T**ag |
| **VTP** | **V**LAN **T**runking **P**rotocol |
| **WAN** | **W**ide **A**rea **N**etwork |
| **WDM** | **W**avelength-**D**ivision **M**ultiplexing |
| **WRR** | Shape-deficit **W**eighted **R**ound **R**obin |
| **XCON-CCM** | cross-**CON**nection **CCM** |

# Safety Requirements

| | |
|---|---|
| ⚠ | **CAUTION!**<br>To reduce risk of physical harm, equipment damage, and fire and to maintain proper operation, ensure that the safety requirements stated hereunder are met! |

## At all Times

Do not let optical fibers come into physical contact with any bare part of the body since they are fragile, and difficult to detect and remove from the body!

Do not look into the end of an optical fiber since it may be carrying harmful laser radiation that can cause permanent damage to the eye and even loss of sight!

Do not bend any part of an optical fiber/cable to a diameter that is smaller than the minimum permitted according to the manufacturer's specification (usually about 65 mm or 2.5 in)!

## Before Installing

**Power** Ensure that *all* power to the OS900 is cut off. Specifically, disconnect the OS900 power cord(s) from the power source (line/mains).

**Inspection** By inspection, ensure that no part of the OS900 is damaged.

**Covers** Leave the protective covers (e.g., dust caps on optical connectors, etc.) on the OS900 components at all times until the components are about to be connected.

**Grounding** For personal protection against electrostatic discharge (ESD), ensure that the OS900 is electrically connected to ground at the butterfly nut on screw (or at the earthing tang) located on the rear (and shown on the right).

**Wrist Strap** For personal and equipment protection against ESD, wear an ESD-protective wrist strap that is connected to ground. The wrist strap must have a resistance of at least one megohm in the path to ground.

**Site** Reserve one of the following sites for the OS900 allowing for, in addition, a clearance of at least 25 mm (1 inch) between the air vents and nearby objects:

- Rack Space:
  - For models OS904/AC-1, OS904/DC-1, OS906/AC-1, OS906/DC-1:
    219.6 x 43.65 x 265 mm$^3$
    [8.45 x 1.72 x 9.45 in$^3$]
  - For models OS906/AC-2, OS906/DC-2:
    443 x 43.65 x 204 mm$^3$
    [17.4 x 1.72 x 8.03 in$^3$]
  - For models OS910/AC-1, OS910/DC-1, OS910/DC-2:
    214.6 x 43.65 x 240 mm$^3$
    [8.45 x 1.72 x 9.45 in$^3$]
  - For models OS910/AC-2:
    316.6 x 43.65 x 240 mm$^3$
    [12.45 x 1.72 x 9.45 in$^3$]
  - For model OS910-M:
    443 x 43.65 x 315 mm$^3$
    [17.44 x 1.72 x 12.4 in$^3$]
  - For models OS912-AC-2, OS912-DC-2:
    443 x 43.65 x 204 mm$^3$
    [17.4 x 1.72 x 8.03 in$^3$]
  - For models OS930:
    443.6 x 43.65 x 290 mm$^3$
    [17.48 x 1.72 x 11.42 in$^3$]

- Wall Area:
    - For models OS904/AC-1, OS904/DC-1, OS906/AC-1, and OS906/DC-1:
      219.6 x 265 mm $^3$
      [8.45 x 9.45 in $^3$]
- Desktop (Flat, stable, non-conductive, static-free surface):
    - For models OS904/AC-1, OS904/DC-1, OS906/AC-1, OS906/DC-1:
      219.6 x 265 mm $^3$
      [8.45 x 9.45 in $^3$]
    - For models OS906/AC-2, OS906/DC-2:
      443 x 204 mm $^3$
      [17.4 x 8.03 in $^3$]
    - For models OS910/AC-1, OS910/DC-1, OS910/DC-2:
      214.6 x 240 mm $^3$
      [8.45 x 9.45 in $^3$]
    - For models OS910/AC-2:
      316.6 x 240 mm $^3$
      [12.45 x 9.45 in $^3$]
    - For model OS910-M:
      443 x 315 mm $^3$
      [17.44 x 12.4 in $^3$]
    - For models OS912-AC-2, OS912-DC-2:
      443 x 204 mm $^3$
      [17.4 x 8.03 in $^3$]
    - For models OS930:
      443.6 x 290 mm $^3$
      [17.48 x 11.42 in $^3$]

# During Installation/Maintenance

Avoid direct exposure to laser beams. In particular, do not look into laser ports.

Ensure that each SFP port at which laser beams are (or will be) present is occupied by an SFP that is locked in position.

# Before Powering On

**Temperature** Operate the OS900 only at a location where the environmental temperature is in the range specified for the model. For details, refer to *Table 1*, page *58*.

**Humidity** Operate the OS900 only at a location where the environmental humidity is non-condensing and between 10 and 85%.

**Dust** Ensure that the site for the OS900 is dust-free. (Less than 1,000,000 particles per cubic meter or 30,000 particles per cubic foot is OK.)

**Cooling Air** Ensure that the airflow around the OS900 and through the air vents is not obstructed. In particular, ensure that there is a clearance of at least 25 mm (1 inch) between the air vents and nearby objects.

**Line Voltage** Ensure that the input voltage to the OS900 from the power source is as follows:
For AC power supply: 90 to 240 Vac (@ 60 to 50 Hz)
For DC power supply: -36 to -72 Vdc.

**Power Cord** The OS900's AC power cord must have one of the following specifications:

***115V AC Power Cord:*** The power cord to be used with a 115 Volt AC configuration must be a minimum type SJT (SVT) 18/3, rated 250 Volts AC, 10 Amps with a maximum length of 4.5 meters (15 feet). One end is terminated in an IEC 320 attachment plug, the other in a NEMA 5-15P plug.

***230V AC Power Cord*:** The power cord to be used with a 230 Volt AC configuration must be a minimum type SJT (SVT) 18/3, rated 250 Volts AC, 10 Amps with a maximum length of 4.5 meters (15 feet). One end is terminated in an IEC 320 attachment plug. The other end is terminated as required by the recognized safety organization of the country in which it is to be installed.

# During Operation

Ensure that each SFP/XFP port at which laser beams are present is occupied by an SFP/XFP that is locked in position.

Do not connect or disconnect cables and/or power cords during lightning strikes or thunderstorms.

# Servicing

All servicing must be carried out only by *qualified* service personnel.

Before servicing, ensure that *all* power to the OS900 is cut off!

# Exigences de sécurité

| | |
|---|---|
| ⚠ | **CAUTION!**<br>Afin de réduire les risques de dommages physiques, dommages du matériel et d'incendie, et afin de maintenir un bon fonctionnement, s'assurer que les exigences de sécurité indiquées ci-dessous sont remplies! |

## À tout moment

Ne pas laisser les fibres optiques entrer en contact physique avec toute partie du corps restée à nu, car elles sont fragiles et difficiles à détecter et à éliminer du corps!

Ne pas regarder directement dans l'extrémité d'une fibre optique car elle risque d'émettre des rayons laser nocifs qui peuvent causer des dommages permanents à l'œil allant jusqu'à la perte de la vue!
Ne plier aucune partie d'une fibre ou d'un câble optique jusqu'à un diamètre inférieur au minimum autorisé selon les spécifications du fabricant (généralement environ 65 mm ou 2,5 po)!

Produit de Laser Classe I. Les lasers internes sont conformes à IEC 60 825-1:1993 + A1:1997 + A2:2001/EN60825-1:1994+A1:1996+A2:2001

Attention: L'utilisation de commandes ou l'adaptation ou l'exécution de procédures autres que celles spécifiées dans ce manuel risquent de résulter en une exposition dangereuse à de la radiation.

## Avant l'installation

| | |
|---|---|
| ***Alimentation*** | S'assurer que *toute* l'électricité allant à l'OS900 est coupée. Plus précisément, débrancher le cordon d'alimentation de l'OS900 de la source d'énergie (enligne/en réseau). |
| ***Inspection*** | Inspecter afin de vérifier qu'aucune partie de l'OS900 n'est endommagée. |
| ***Couvercles*** | Laisser les couvercles protecteurs (c'est à dire les tapes contre la poussière sur les connecteurs optiques, etc.) sur les éléments de l'OS900 à tout moment jusqu'à ce que les éléments soient sur le point d'être connectés. |
| ***Mise à la terre*** | Pour la protection du personnel contre les décharges électrostatiques (ESD), s'assurer que le OS900 est relié électriquement à la terre à l'écrou papillon qui se trouve sur la vis située à l'arrière. |

# Chapter 1: Overview

## General

The OS900 is a multi-layer Telco-compliant compact carrier-class Ethernet demarcation services platform that provides Layer 2 and 3 functionality.

It enables premium manageable Ethernet services with extensive traffic management and end-to-end control for service-level conformance.

The OS900 functions as a demarcation device at the customer's premises and is owned by the service provider. It provides a carrier-to-customer User-Network Interface (UNI) that separates the carrier's WAN from the customer's LAN to free the provider of the need to configure the customer's LAN/devices. The OS900 enables bandwidth limiting, security, and monitoring of customer and network interfaces with clear visibility of LAN and WAN segments.

For inter-provider demarcation points, the OS900 serves as a demarcation device at the carrier-to-carrier on-net locations, and provides Network-Network Interfaces (NNI) that separate two different service provider networks. In such an application, the OS900 enables Ethernet service delivery over multiple carrier transport networks with end-to-end visibility and control.

## Product Highlights

- Service demarcation for Metro Ethernet E-Line, E-LAN, and EPL connectivity services:
  - MEF 9[3] service conformance
  - Provider bridging or MPLS L2 VPN services
  - Service protection (with 50 ms recovery time)
- H-QoS according to MEF 14[4] Traffic Management conformance
- Ethernet Service OAM to guarantee SLAs
- Multi-purpose customer & network interfaces at lower TCO
- IPv6 future proof (hardware enabled)
- Unified Master-OS™ control plane across all models
- Circuit Emulation and MPLS Services
- Wirespeed Routing
- CPU and FPGA tests supported (by the nbEthOamCapabilities object in the private MIB nbEthOam.mib)

## Applications

- Micro-PoP Services
- Business Ethernet Services
- Intra-provider and Inter-provider WAN Ethernet Manageable Services (Ports can serve as UNIs or NNIs)

## Architecture

With state-of-the-art wire-speed technology, the OS900 offers a future-proof solution for ILECs, IXCs, MSOs, or green-field service providers to meet various business subscriber SLA

[3] Test suite for Ethernet services at the UNI

[4] A standard defining the requirements and corresponding test procedures for Service Performance and Bandwidth Profile Service Attributes that may be specified as part of a Service Level Specification (SLS) for an Ethernet Service

requirements. A single OS900 serving as a demarcation device can facilitate the provisioning of revenue generating new value-added services thanks to its wide spectrum of service features.

# Telco Compatibility

All models of the OS900 can be mounted in standard 19-inch and 23-inch Telco racks. Models OS904, OS906, and OS910 with a single power supply can be mounted side-by-side in pairs in a single 19-inch or 23-inch Telco rack frame to enable OS900 protection, high port density, as well as easy accessibility.

# Optical SFP Interfaces

SFP interfaces provide unmatched deployment flexibility to enable versatile optical extensions from short to long-haul singlemode, single-fiber, or CWDM/DWDM connections – simply by use of an appropriate SFP.

For service providers who build next-generation optical networks, the consolidation of xWDM services with intelligent traffic forwarding on the same platform offers significant savings in capital expenditure.

The integration of CWDM and DWDM SFPs eliminates the need for a transponder on the network, and offers increased fiber optimization with physical services separation and dedicated Gigabit rate for premium optical services based on the same concept of legacy “leased-line” services.

# VPN Services & Protection

Compliant to MEF Ethernet Virtual Circuit (EVC), the OS900 offers three types of VPN service:

1. Layer 1 Optical VPN (Media Cross-Connect) – a cross-connect mode with transparent mode (without MAC address learning). This type of VPN functions like an *intelligent* patch panel. In typical patch panels, wires must be physically disconnected, moved, and reconnected to change the network configuration. In the OS900, physical connections are left unchanged; only logical connections are changed – purely by software control – to give the desired port-to-port interconnections. One application of Media Cross-Connect is to forward data via a WDM technology port.
2. Layer 2 VPN – VLAN-based tunneling Q-in-Q stacking, swapping, or mapping services.
3. Layer 2.5 VPN – a label-based MPLS VC for direct connection into MPLS domains or H-VPLS MTUs.

All the above VPN services can be fully protected using port protection, dual-homing, and/or ring topology with a recovery time of less than 50 ms.

In addition to L2 VPN, the OS900 offers Layer 3 integrated IP router services to save on costs for an external router and functions as a single demarcation platform for managed L2 VPN and IP services.

# Traffic Management

The OS900 provides for a value-added network infrastructure with end-to-end per-flow QoS.

It supports full CoS and QoS (MEF 14 model) including flow classification, rate limiting, shaping, WFQ scheduling, and strict priority scheduling for lower delay/jitter, and guaranteed throughput in real-time applications. In addition, it enables dynamic/adaptive buffer pools to prevent bursty traffic starvation for buffers while ensuring effectiveness of queuing resources.

For network convergence applications that have a clear boundary between a customer’s network and the carrier’s network, CoS layers (802.1p) can be mapped/marked to preserve priorities or mapped into protection profiles preconfigured by the carrier.

# Hierarchical QoS – CoS-Aware Rate Limit

Defining premium SLAs is a key requirement for service differentiation.

The OS900 enables traffic management based on innovative CoS-aware rate limit to dynamically use available bandwidths. Dynamic QoS enables sharing of defined rate-limited flows controlled by an aggregate profile configured for a UNI or an Ethernet Virtual Circuit. In the new service offering, consolidated real-time, high-priority, and best effort require the options of differing data rates configuration and CoS remarking. Dynamic QoS provides for sharing/borrowing bandwidths allocated for real-time or high-priority applications at intervals when these services are in standby. This capability optimizes bandwidth utilization at the access/demarcation point of the network without the need for involving the aggregation layer for this purpose.

# Denial of Service (DoS) Protection

The OS900 incorporates multi-layer DoS protection at the hardware level on the CPU control plane and data-switching plane to protect service and device functionality from hostile traffic without causing degradation of service performance or affecting the forwarding database or CPU availability. Multiple traffic types can be policed at Layer 2 (e.g., broadcast frames, multicast frames), Layer 3 (e.g., IP, OSPF), and Layer 4 (e.g., TCP, UDP).

# System Management

The OS900 control plane incorporates a range of highly manageable features that offer assured interaction with carriers' OSS and NMS platforms, based on industry-standard Southbound out-of-band or in-band interfaces. In addition, it can be managed with MRV's MegaVision Pro NMS to provide complete GUI and Northbound gateway (XML, TL1 & SNMP) to an entire cluster of devices for configuration, performance analyses, and inventory control.

For the service provider, the OAM that is provided by a demarcation device determines to a significant extent the metrics that can be used to formulate the SLA in cooperation with a service subscriber.

The OS900 incorporates enhanced standards-compliant MEF OAM and gives the service provider the capability to monitor the network, provision services, and promptly isolate fault locations from a remote network operation center.

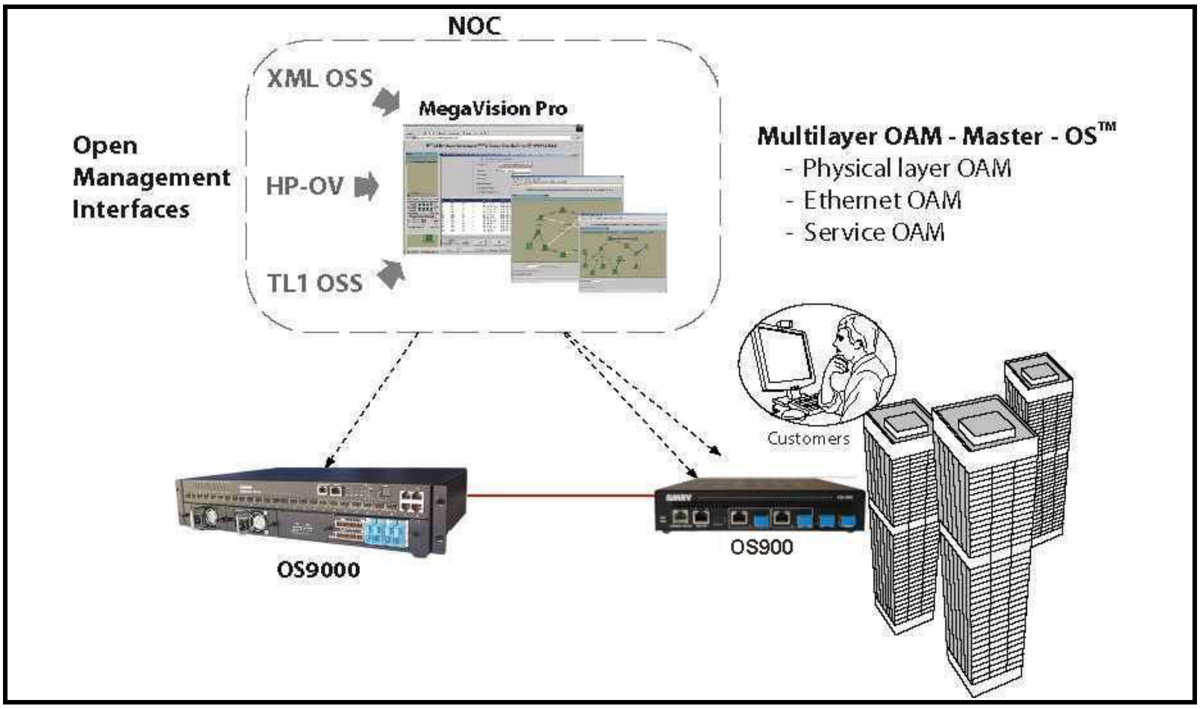



**Figure 1: Operations, Administration, and Maintenance**

# Ethernet OAM with IEEE 802.1ag and ITU-T Y.1731

Connectivity of Ethernet bridging devices across Metro Ethernet or other transport networks provides virtual (dedicated) Ethernet circuits. End-to-end service architecture requires administrative domain hierarchy with corresponding OAM-enabled titles. The OS900 incorporates such connectivity, discovery, and fault management along with performance statistics on delay, jitter, and frame loss for demarcation and intermediate points of service.

# Ethernet OAM with IEEE 802.3ah

IEEE 802.3ah Ethernet OAM provides reliable service assurance mechanisms for provider as well as customer networks so as to avoid expensive time-consuming in-the-field truck rolls for isolating faults. It includes Discovery Process, Dying Gasp, and Remote Loopback.

# Ethernet Loopbacks

The OS900 offers remote loopback functionality on a physical interface or a specific VLAN that traverses UNI or NNI interfaces. The loopback function allows for remote troubleshooting of services, from NOC or any other manageable location without having to actually visit the customer premises. Loopback functionality is hardware controlled to provide performance monitoring and SLA verification at wire speed.

# Virtual Cable Diagnostics

The OS900's Virtual Cable Diagnostics (VCD) feature enables the administrator to test electrical data cables attached to its ports for a physical fault, to identify the fault type, and to pinpoint its location – all this with a single command. The technology used in devising VCD is Time-Domain Reflectometry (TDR), which works on the same principle as radar.

In Ethernet networks, Layer 1 and Layer 2 elements are so closely coupled that it is often impossible to determine at what layer the fault is present. Without VCD, isolation of the fault would involve rollouts of burdensomely numerous cables and other equipment without knowing what or where the fault is, thereby dramatically increasing maintenance costs and downtime!

Faults that can be detected with VCD are: opens, shorts, bad connectors, impedance mismatch, and polarity mismatch.

# Digital Diagnostics (Optical Performance Level Monitoring)

The digital diagnostics feature of the OS900 SFPs (as per the standard SFF-8472) serves as a powerful OPM tool that provides access to a number of real-time SFP operating parameters such as optical Tx/Rx power, voltage, and temperature, as well as component information, such as, vendor code, serial number, and wavelength. The information provided using digital diagnostics, together with alarm and warning thresholds, enables the network administrator to identify potential problems in optical transmission and take preemptive action before any service outage actually occurs.

# Link Aggregation

The IEEE802.3ad Link Aggregation Control Protocol provides a way to set up an aggregation trunk automatically between two peers. The protocol controls bundling of several physical ports together to form a single logical channel.

Unlike LAG which requires the configuration to be defined statically, LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.

Such a channel between two switches increases traffic throughput capacity among stations connected to the ports that are members of the trunk. For example, the interconnection of eight full-duplex Gigabit ports of one OS900 unit to eight full-duplex Gigabit ports of another OS900 unit, serves as an 8-Gbps full-duplex Ethernet trunk.

# Per-service Performance Monitoring

The OS900 provides real-time and history reporting on various service performance metrics, including port/VPN-EVC utilization, transmission errors, and QoS threshold exceptions.

Each service can be tracked for statistical information to help in baselining and troubleshooting traversing services. This capability enables users to verify service guarantees and increase network reliability by validating network performance. Performance monitoring uses proactive monitoring to regulate traffic in a continuous, smooth, reliable, and predictable manner so as to enable measurement of network performance and health.

# Link Reflection/Propagation

The Link Reflection/Propagation mechanism provides notification on the integrity of a link from the network interface to the user interface even if the link extends through *several* OS900s.

# Analyzer VLAN

The OS900 incorporates the powerful Analyzer VLAN feature. This feature enables the operator to configure a dedicated Analyzer VLAN for remote analysis by a surveillance center. It can be activated per customer VLAN, per L2, L3, or L4 fields, or per learn table MAC address. The remote service monitoring conforms with the interception processes according to the requirements of Law Enforcement Monitoring.

# Multiple-instance STP

Multiple-instance STP (MSTP) allows for the creation of multiple STP instances concurrently on a network with network inter-node links that can be shared by any number of instances. The implementation complies with the IEEE 802.1**s** standard and is backward compatible with the spanning-tree protocols STP (IEEE 802.1**d** standard) and RSTP (IEEE 802.1**w** standard) so that the OS900 can be used in a network consisting of devices operating in STP, RSTP, and MSTP.

MSTP serves to:

1. Prevent collapse of communication over a network whose topology is changed dynamically.
2. Address the needs of increasingly faster Ethernet networks with mission-critical applications requiring quick convergence/recovery. (The convergence/recovery time is 50 to 200 ms, the actual time depending on the network).
3. Maximize traffic flow across a network by optimizing resource utilization (for e.g., by utilizing unused inter-node links).
4. Balance traffic flow across the network in order to increase throughput.
5. Improve fault tolerance by enabling traffic to flow unaffected in MSTIs even when failure occurs in one or more other MSTIs.

# Models

The OS900 is available in various models with flexibly selectable SFPs so that a model and SFPs that are most suitable to an application can be selected. The models are described in *Table 1*, below. The SW-UPG-9xMPLS enhanced software upgrade package (Master-OS™: MPLS VC - LDP, RSVP-TE, CR-LDP, OSPF-TE, CSPF) option can be ordered with an OS900 model. Models with this option are referred to with the character "S" appended to the model name, e.g., OS910-MS.

**Table 1: Models of the OS900**

| Model | Description |
|---|---|
| **Regular Operating Temperature (0 to 50 °C or 32 to 122 °F) Models** | |
| OS904/AC-1 | Intelligent Ethernet services demarcation platform with 2 x Tri-mode[5] ports (100FX/1000FX SFP or RJ45 10/100/1000Base-T) + 2 x 100/1000Base-X SFP ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 1 x built-in AC power supply (90-240 Vac) + 1 x pair of 19-inch rack-mount brackets.<br>Two OS904/AC-1s are side-by-side mountable on a wall or in a Telco 19-inch or 23-inch rack. |
| OS904/DC-1 | Like the OS904/AC-1 except that it has a DC power supply (-48 Vdc) instead of an AC power supply. |
| OS904/DC-1N | Like the OS904/DC-1 except that its DC power supply is -24 Vdc. |
| OS904/DSL4 | Like the OS904/AC-1 except that it can concurrently also function as a Single-pair High-speed Digital Subscriber Line (SHDSL) transceiver. The DSL port has 4 DSL channels. |
| OS904/DSL4D | Like the OS904/DSL4 except that it has a DC power supply instead of an AC power supply. |
| OS906/AC-1 | Intelligent Ethernet services demarcation platform with 6 x Tri-mode ports (100FX/1000FX SFP or RJ45 10/100/1000Base-T) + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 1 x built-in AC power supply (90-240 Vac) + 1 x pair of 19-inch rack mount brackets. Two OS906/AC-1s are side-by-side mountable on a wall or in a Telco 19-inch or 23-inch rack. |
| OS906/AC-2 | Intelligent Ethernet services demarcation platform with 6 x Tri-mode ports (100FX/1000FX SFP or RJ45 10/100/1000Base-T) + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 2 x built-in AC power supplies (90-240 Vac) + 1 x pair of 19-inch rack-mount brackets. Mountable in Telco 19-inch or 23-inch rack. |
| OS906/DC-1 | Like the OS906/AC-1 except that it has a DC power supply (-48 Vdc) instead of an AC power supply. |
| OS906/DC-1N | Like the OS906/DC-1 except that its DC power supply is -24 Vdc. |
| OS906/DC-2 | Like the OS906/AC-2 except that it has two DC power supplies (-48 Vdc) instead of AC power supplies. |
| OS906/DC-2N | Like the OS906/DC-2 except that its DC power supplies are -24 Vdc. |
| OS906/ACDC-2 | Intelligent Ethernet services demarcation platform with 6 x Tri-mode ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 2 x built-in mutually redundant power supplies (90-240 Vac and –48 Vdc) + 1 x pair of 19-inch rack-mount brackets. Mountable in Telco 19-inch or 23-inch rack. |
| OS910/AC-1 | Intelligent Ethernet services demarcation platform with 8 x 10/100/1000Base-T ports (fixed) + 2 x 100/1000Base-X hot-swappable SFP ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 1 x built-in AC power supply (90-240 Vac) + 1 x pair of 19-inch rack-mount brackets.<br>Two OS910/AC-1s are mountable on a wall or in Telco 19-inch and 23-inch racks. |
| OS910/AC-2 | Intelligent Ethernet services demarcation platform with 8 x 10/100/1000Base-T ports (fixed) + 2 x 100/1000Base-X hot-swappable SFP ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 2 x built-in AC power supplies (90-240 Vac) + 1 x pair of 19-inch rack-mount brackets. |
| OS910/DC-1 | Like the OS910/AC-1 except that it has a DC power supply (-48 Vdc) instead of an AC power supply. |
| OS910/DC-2 | Like the OS910/AC-2 except that it has a two DC power supplies (-48 Vdc) instead of two AC power supplies. |

[5] Tri-mode ports can operate in either of the following Ethernet protocols: 10/100/1000Base-T, 100Base-FX, or 1000Base-X.

**Table 1: Models of the OS900** (Cont'd)

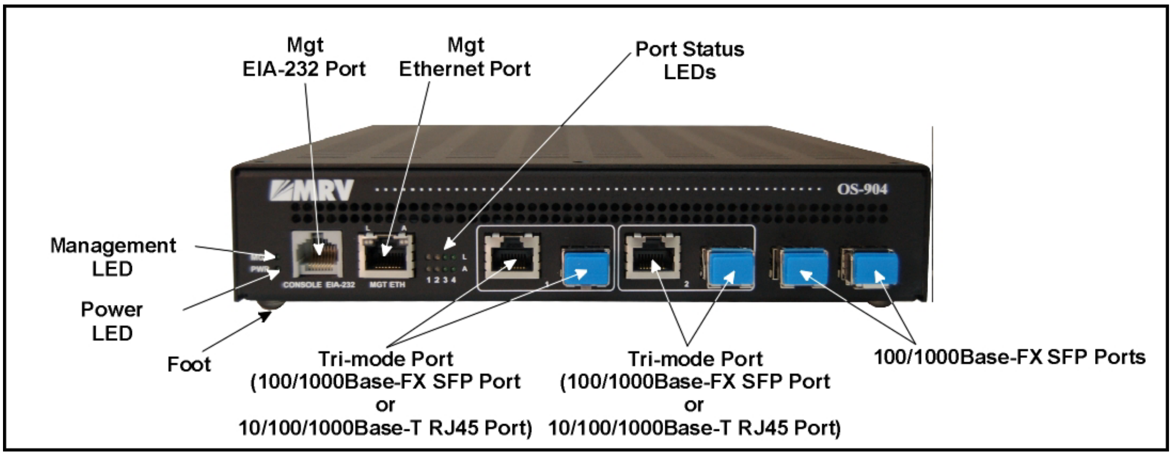
| Model | Description |
|---|---|
| **Regular Operating Temperature (0 to 50 °C or 32 to 122 °F) Models** (Cont'd) | |
| OS910-M | Mini multi-service modular platform with 6 x 10/100/1000Base-T ports (fixed) + 2 Tri-mode ports + 2 x 100/1000Base-X hot-swappable SFP ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 2 optional service modules (e.g., WDM, E1/T1) + 1 x pluggable, hot-swappable power supply or 2 x pluggable, mutually redundant, hot-swappable power supplies + 1 x pair of 19-inch rack-mount brackets.<br>Part number of 90-240 Vac *AC* power supply: EM9-M-PS/AC.<br>Part number of -48 Vdc *DC* power supply: EM9-M-PS/DC.<br>Part number of -24 Vdc *DC* power supply: EM9-M-PS/24DC<br>Mountable in Telco 19-inch or 23-inch racks. |
| OS912-AC-2 | Intelligent Ethernet services demarcation platform with 12 Tri-mode ports + 2 x AC power supplies + 1 x pair of 19-inch rack-mount brackets.<br>Brackets for mounting in a 19-inch rack included. |
| OS912-DC-2 | Like the OS912-AC-2 except that it has a two DC power supplies (-48 Vdc) instead of two AC power supplies. |
| OS930 | Intelligent Ethernet services demarcation platform with 3 x **10 Gbps Ethernet** hot-swappable XFP ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 1 x pluggable, hot-swappable power supply or two pluggable, hot-swappable, mutually redundant, power supplies (Part number of *AC* power supply (90-240 Vac): EM9005-PS/AC. Part Number of *DC* power supply (-48 Vdc): EM9005-PS/DC) + 1 x pair of 19-inch rack-mount brackets.<br>Mountable in Telco 19-inch or 23-inch racks. |
| **Extreme Operating Temperature (-10/-40 to 65 °C or 14/-40 to 149 °F) Models** | |
| OS904E/AC-1 | Intelligent Ethernet Services Demarcation with *high* temperature support (-10 to 65 °C) with 2 x Tri-Mode (100FX/1000FX SFP or RJ45 10/100/1000Base-T) + 2 x 100FX/1000FX SFP Ports + 1 x out-of-band management RS-232 port + 1 x out-of-band management Ethernet port + 1 x built-in AC power supply (90-240 Vac) + 1 x pair of 19-inch rack-mount brackets.<br>Two OS904E/AC-1s are side-by-side mountable on a wall or in a Telco 19-inch or 23-inch rack. |
| OS904E/DC-1 | Like the OS904E/AC-1 except that it has a DC power supply (-48 Vdc) instead of an AC power supply. |
| OS904E/DC-1N | Like the OS904E/DC-1 except that its DC power supply is -24 Vdc. |
| OS904EXT/AC-1 | Intelligent Ethernet Services Demarcation with *extreme* temperature support (-40 to 65 °C) with 2 x Tri-Mode ports (100FX/1000FX SFP or RJ45 10/100/1000Base-T) + 2 100FX/1000FX SFP ports + 1 x AC power supply (220 Vac) ) + 1 x pair of 19-inch rack-mount brackets.<br>Two OS904EXT/AC-1s are side-by-side mountable on a wall or in a Telco 19-inch or 23-inch rack. |
| OS904EXT/AC-1N | Like the OS904EXT/AC-1 except that its AC power supply is 110 Vac. |
| OS904EXT/DC-1 | Like the OS904EXT/AC-1 except that it has a DC power supply (-48 Vdc) instead of an AC power supply. |
| OS904EXT/DC-1N | Like the OS904EXT/DC-1 except that its DC power supply is -24 Vdc. |

# Layout

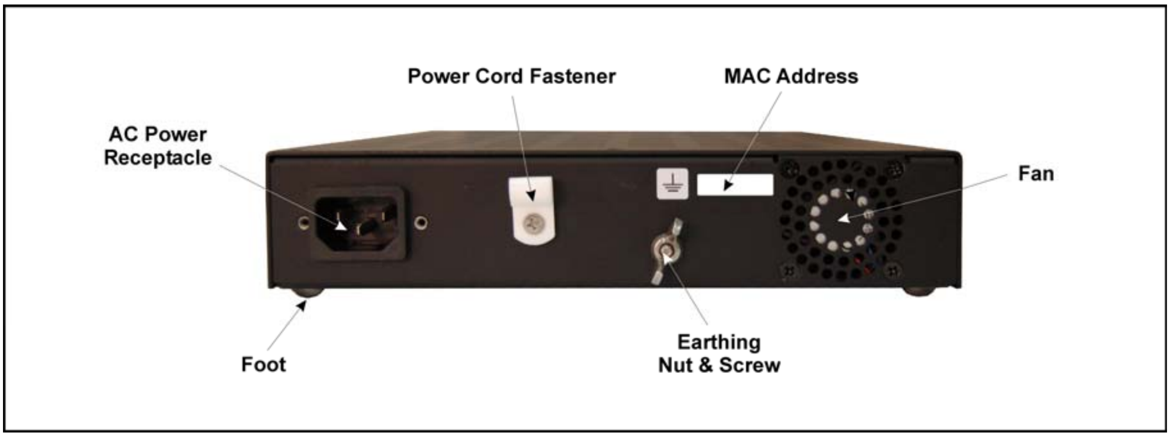
## View

The layout of the OS900 is shown in *Figure 2*, below.

### OS904/AC-1

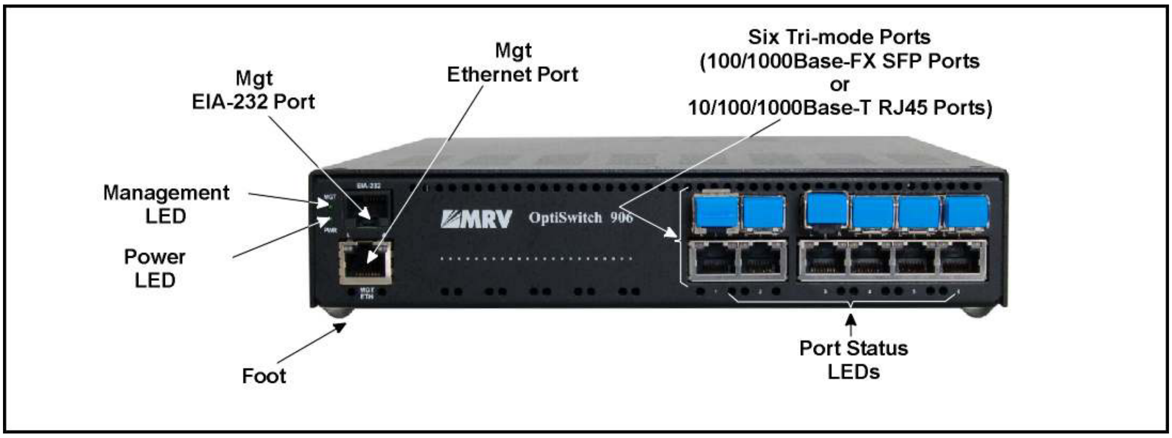



**Front**

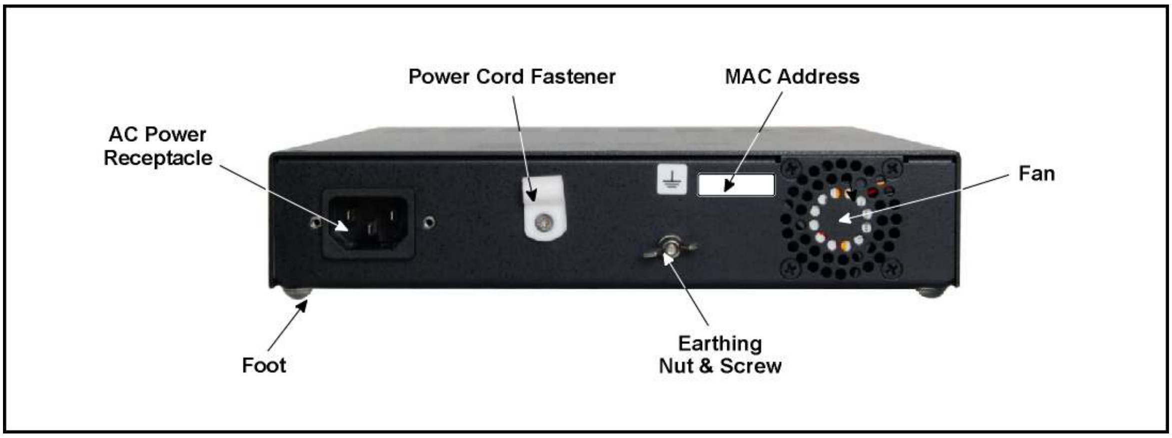



**Rear**

### OS906/AC-1

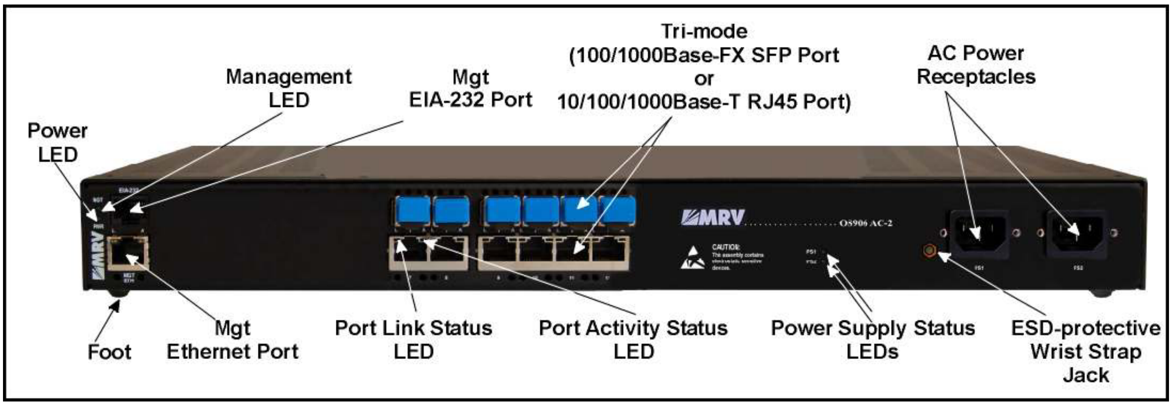



**Front**




**Rear**

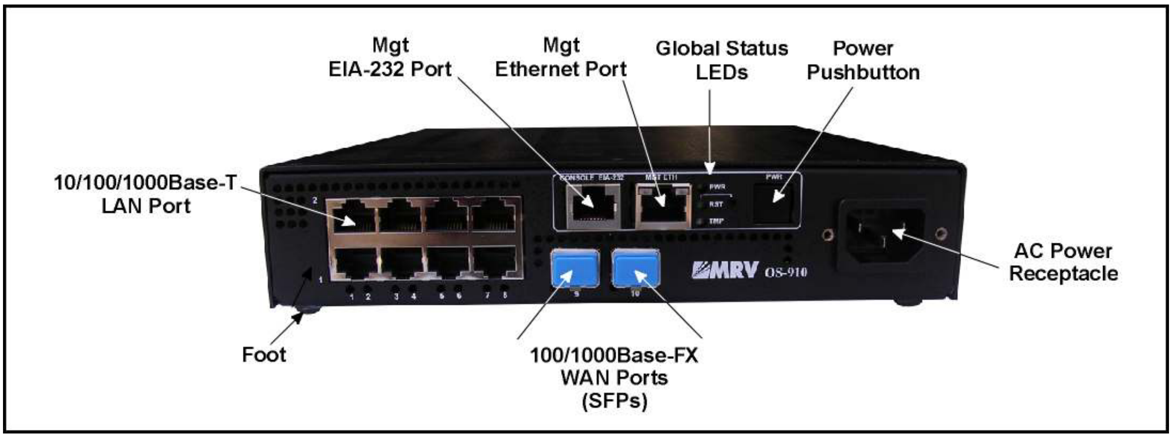
## OS906/AC-2



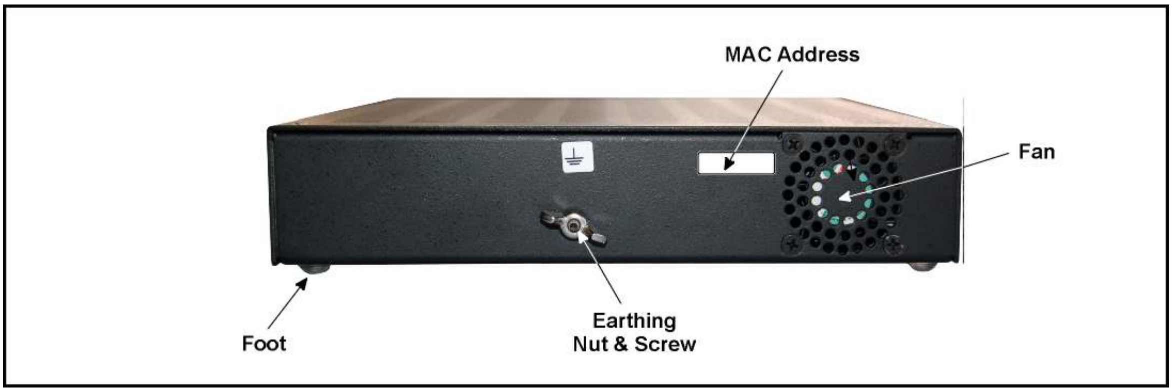

**Front**


**Rear**

## OS910/AC-1

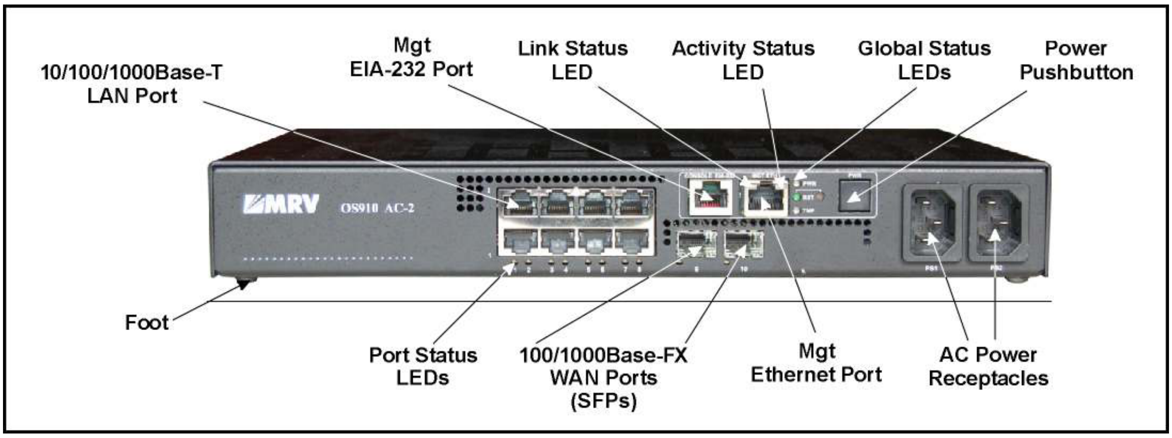



**Front**

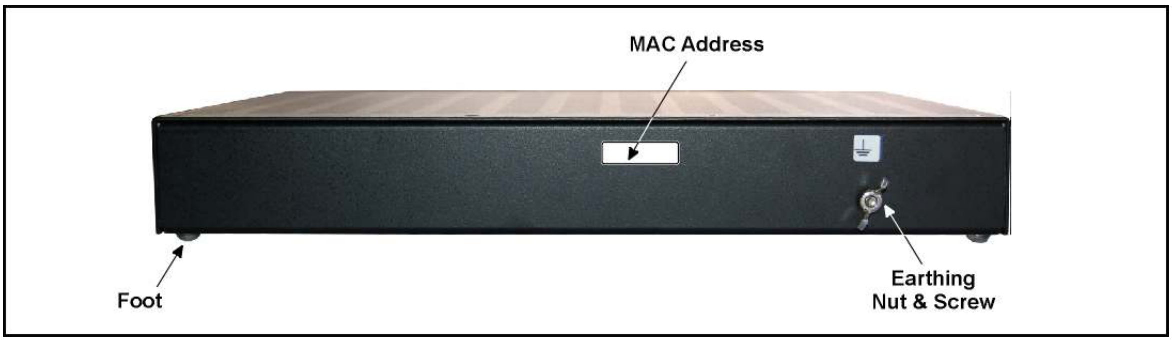



**Rear**

**OS910/AC-2**

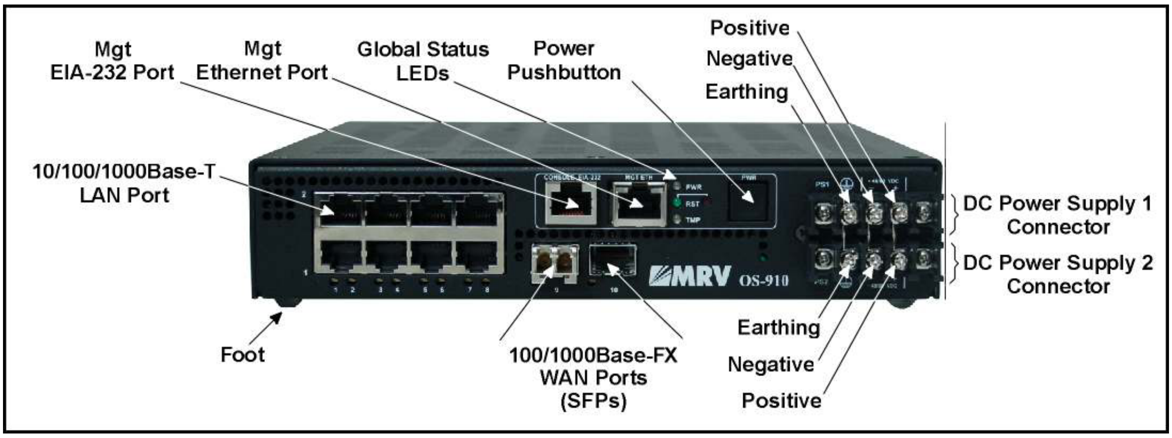



**Front**

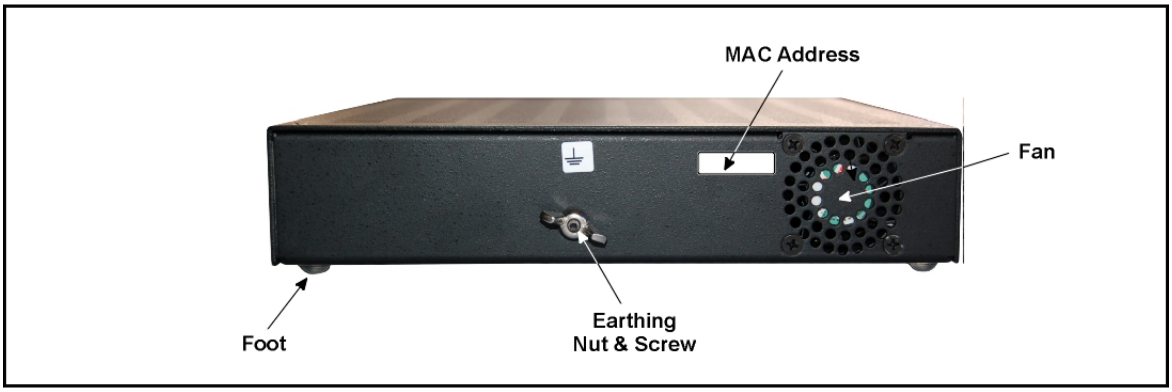



**Rear**

**OS910/DC-2**

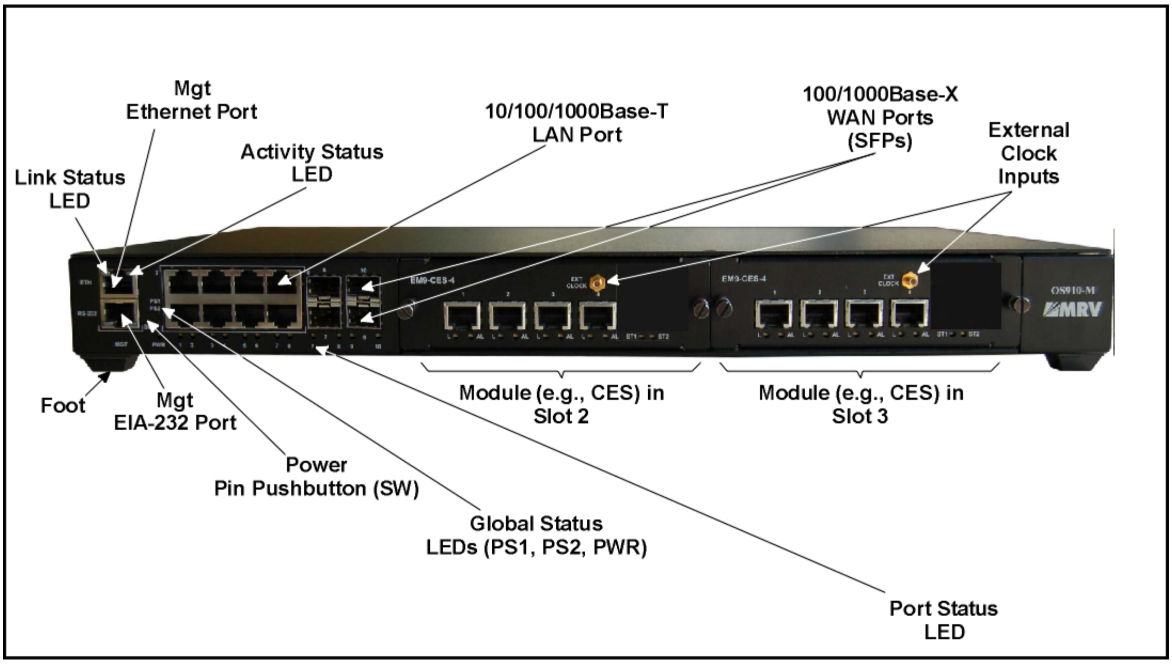



**Front**

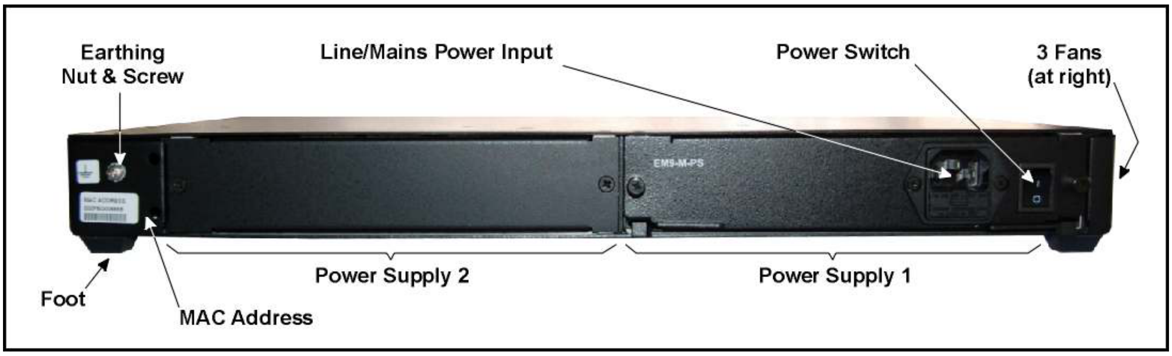



**Rear**

## OS910-M

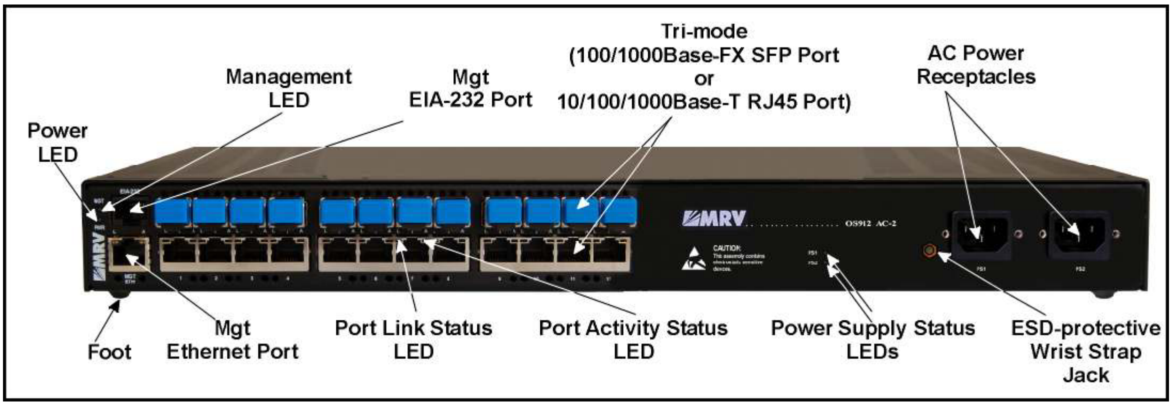



**Front**




**Rear**

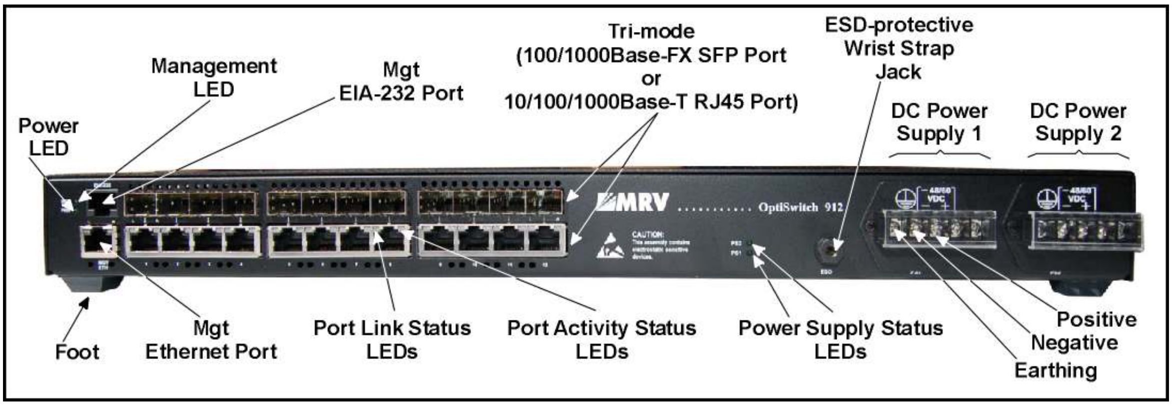
**OS912-AC-2**




**Front**


**Rear**

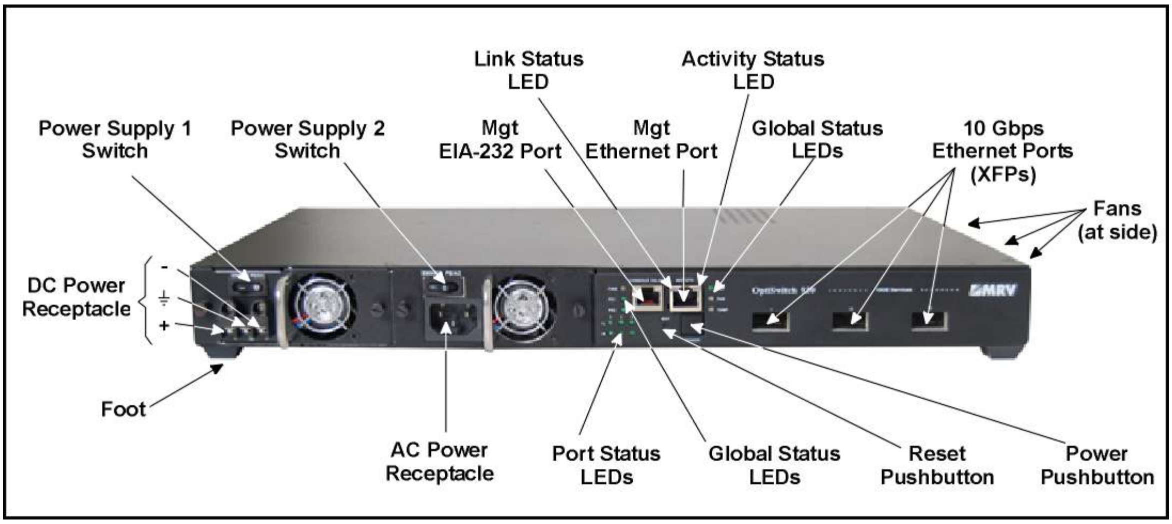
**OS912-DC-2**




**Front**


**Rear**

**OS930/AC**




**Front**


**Rear**

**Figure 2: Layout of OS900**

## Power Supply Switch (Only in OS910-M and OS930)

Power supply switch 0 I.
I Position: Allows power into the OS900; O Position: Prevents power into the OS900.

## Power Pushbutton

OS910-M Model
Pin pushbutton ***SW*** for powering ON/OFF the OS910-M system.
Other Models
Pushbutton ***PWR/POWER*** for powering ON/OFF the OS900 system.

## Reset Pushbutton (Not in OS910-M)

Pin pushbutton ***RST*** for restarting the OS900 system.

## External Clock Input (Only in OS910-M)

Jack for connecting an external clock (optional) to the EM9-CES module that may clock transmission of E1/T1 signals with greater precision.

## Ports

Each port can be independently configured to operate in any of a wide range of modes.

For detailed information on configuration of ports, refer to ***Chapter 6:*** *Ports*, page *127*.

**OS904/AC-1, OS904/DC-1**

Two Tri-mode ports (Ports 1 and 2) and two 100/1000Base-X SFP ports (Ports 3 and 4).

**OS906/AC-1, OS906/AC-2, OS906/DC-1, OS906/DC-2**

Six Tri-mode ports (Ports 1 to 6).

**OS910/AC-1, OS910/AC-2, OS910/DC-1, OS910/DC-2**

Eight fixed 10/100/1000Base-T ports (Ports 1 to 8) and two 100/1000Base-X Ethernet SFP ports (Ports 9 and 10).

**OS910-M**

Six fixed 10/100/1000Base-T ports (Ports 1 to 6), two Tri-mode ports (Ports 7 and 8), and two 100/1000Base-X Ethernet SFP ports (Ports 9 and 10).

**OS912-AC-2, OS912-DC-2**

Eight fixed 10/100/1000Base-T ports (Ports 1 to 8), two 100/1000Base-X Ethernet SFP ports (Ports 9 and 10), and two 1000Base-X Ethernet SFP ports (Ports 11 and 12).

**OS930**

Three 10 Gbps Ethernet XFP ports (Ports 1 to 3).

**Management**

***CONSOLE EIA-232***

Serial/RS-232 port (with baud rate 9600 baud) for out-of-band local connection of a craft terminal.

***MGT ETH***

Ethernet 10/100Base-TX port for TELNET, SSH, and/or SNMP *out-of-band* connection. It is directly connected to the CPU and does not affect nor is affected by inband traffic. It is an IP interface that is used only for connecting a management LAN. Management stations on the LAN can be used to manage the OS900 *out-of-band* (using a TELNET, SSH, or SNMP connection over Ethernet). Alternately, a TFTP client can be connected to the out-of-band interface to access configuration files stored in the OS900.

## LEDs

Global and per-port status-indicator LEDs. The LEDs are described in *Table 5*, page *84*.

## Fans

The number of cooling fans in each OS900 model type is shown in *Table 2*, below.

**Table 2: Fans in OS900 Models**

| **Models** | OS904/AC-1, OS904/DC-1, OS906/AC-1, OS906/DC-1, OS910/AC-1, OS910/DC-1, OS910-M/AC-1, and OS910-M/DC-1 | OS906/AC-2, OS906/DC-2, OS910/AC-2, OS910/DC-2, OS910-M/AC-2, OS910-M/DC-2, OS912-AC-2, and OS912-DC-2 | OS930 |
|---|---|---|---|
| **Fans** | 1 | 2 | 4 |

## Earthing

**OS906/AC-2, OS906/DC-2, OS912-AC-2, and OS912-DC-2**

Metal tang at rear for earthing the OS906/AC-2, OS912-AC-2, and OS912-DC-2 chassis.

**OS904, OS906/AC-1, OS906/DC-1, OS910, OS910-M, and OS930**

Butterfly nut on screw (type NC6) at rear for earthing the OS900 chassis.

## Power Supply

For details on the power supply and power consumption, refer to ***Appendix F:*** *Product Specification*, page *813*.

# Options

## SFPs/XFPs

OS930

Fiberoptic 10 GE XFP transceivers can be fitted to Ports 1 to 3 of the OS930.

Others

The ports of OS900 models to which fiberoptic Fast Ethernet/1GE SFP transceivers can be fitted are shown in *Table 3*, below.

**Table 3: SFPs Pluggable in Ports of each OS900 Model**

| **Model** | OS904/AC-1, OS904/DC-1 | OS906/AC-1, OS906/AC-2, OS906/DC-1, OS906/DC-2 | OS910/AC-1, OS910/AC-2, OS910/DC-1, OS910/DC-2 | OS910-M | OS912-AC-2, OS912-DC-2 |
|---|---|---|---|---|---|
| **Ports** | 1 to 4 | 1 to 6 | 9 and 10 | 7 to 10 | 1 to 12 |

## Service Modules (Only in OS910-M)

Up to two service modules may be fitted in the OS910-M model. The types of service module available are:

**WDM Module**– A passive device for adding or dropping optical data carrier wavelengths. The device can be an OADM, Multiplexer, or Demultiplexer module. For details, refer to ***Chapter 37:*** *WDM Module*, page *623*.

**E1/T1 Module**– A TDM for carrying voice on E1/T1 channels over Ethernet. For details, refer to ***Chapter 38:*** *E1/T1 CES* Module, page *629*.

**STM-1/OC3 Module**– A TDM for carrying voice on E1/T1 channels over Ethernet. For details, refer to ***Chapter 39:*** *STM-1/OC3 CES Module*, page *677*.

## Power Supply

OS900s with an additional universal AC or DC power supply are available. The two power supplies operate in mutual redundancy mode. This mode of operation has two advantages:

– First, if one power supply fails, the other will supply the requisite power for continued smooth operation of the OS900. The failure status is recorded in the OS900. The failure status can be viewed using the command **`show version`**.

– Second, the service provider can coordinate the downtime for OS900 maintenance with the customer.

# Chapter 2: Applications

## General

This chapter gives examples of how the OS900 can be applied.

## Micro-PoP Services

*Figure 3*, below, shows how several customers on the same premise can be connected with an OS900, which can be connected to a metro network via the OS9000 aggregation platform.

VLANs can be configured to isolate users from one another if required and to provide Q-in-Q Service VLANs and security.

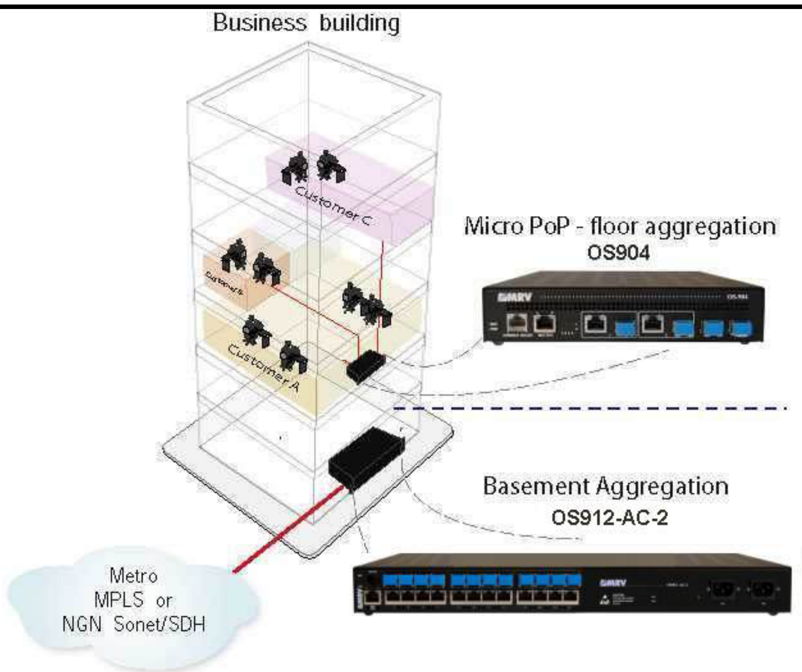



**Figure 3: Micro-PoP Services**

## WAN Ethernet Manageable Services

*Figure 4*, below, shows how OS900s can be used to interconnect WANs of various operator networks.

Q-in-Q (stacked VLANs) can be used to isolate different types of traffic from one another or to bridge customers or groups of customers scattered across the operator's network.

Uplink protection (connection of a dual 100 Mbps or 1G uplink between the OS900 and the same WAN) and/or dual-homing (connection of a dual 100 Mbps or 1G uplink to different WANs) can be implemented.

To provide SLA management and CFM, Traffic Conditioners (TCs) running dynamic CoS can be set up together with ingress and egress traffic shaping.

MRV's MegaVision Pro SNMP network management application can be used on various platforms for management of the OS900 (and other SNMP-manageable devices) via a LAN or the World-Wide Web (WWW).

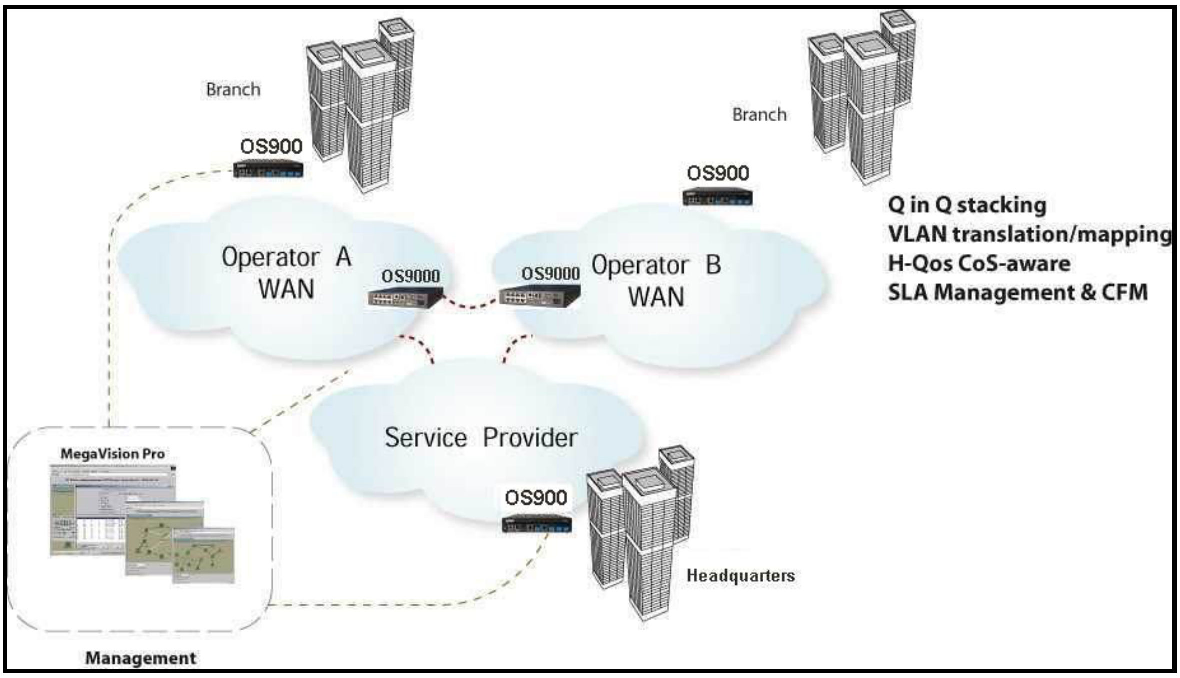



**Figure 4: WAN Ethernet Manageable Services**

# Business Ethernet Services

*Figure 5*, below, shows an application for providing on-premise Ethernet services while freeing the aggregation network segment from the task of handling traffic between the hosts on the segment.

VLANs can be configured to isolate users from one another if required and to provide Q-in-Q Service VLANs and security.

A 100 Mbps or 1 Gbps uplink can be used to connect the OS900 network to the aggregation network segment.

In addition, digital diagnostics per the SFF-8472 standard can be performed for SFP transceivers of the OS900. Layer 1 cable diagnostics (VCD) can be performed to identify and locate faults in copper cables/connections.

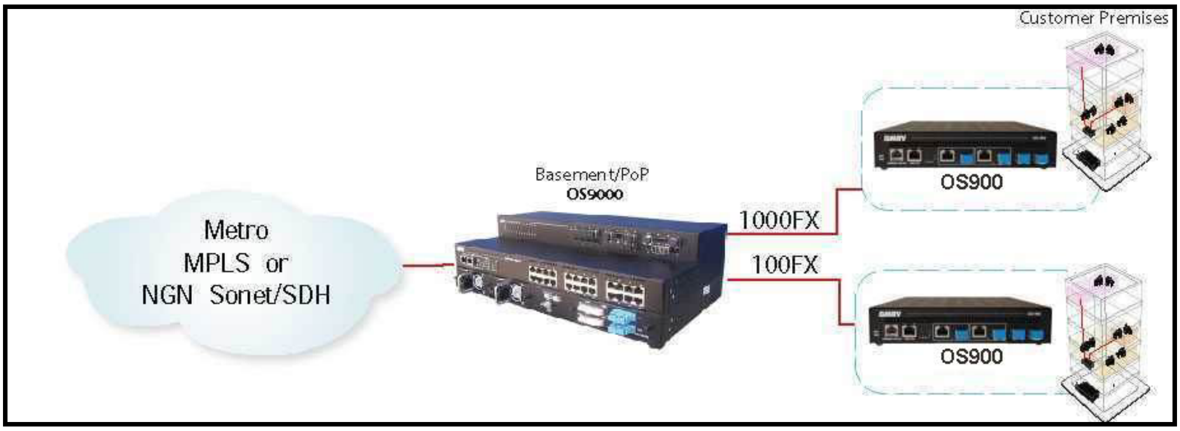



**Figure 5: Business Ethernet Services**

# 10 Gbps Ethernet High-end Demarcation Services

*Figure 6*, below, shows an application for providing mission critical revenue generating 10GE managed Ethernet services.

OS930 interfaces can be configured as UNI or NNI as per MEF specifications and enable the following networking functions:

– 1:1 or 1+1 protected modes with 50 ms restoration time - Ring/Mesh, LIN, and end-to-end protection based on OAM CCM
– Hierarchical QoS traffic management with 10GE subrates (CIR/EIR)
– Ethernet service OAM - SLA management based on CFM IEEE802.1ag and ITU-T Y.1731 PM
– 10GE WAN PHY (WIS) mode - configurable to operate at 10GE, OC192, or STM-64

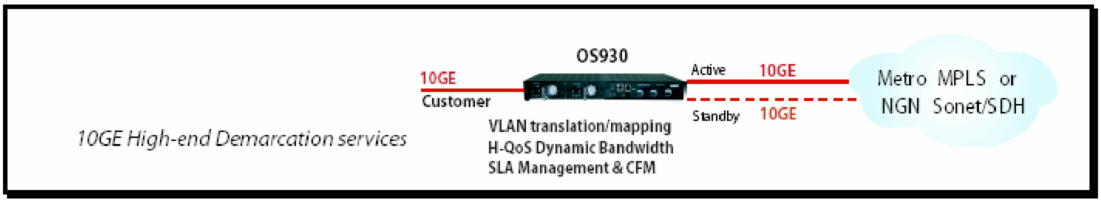



**Figure 6: 10 Gbps Ethernet High-end Demarcation Services**

# WAN 10 Gbps Manageable Ethernet Services

*Figure 7*, below, shows an application for providing manageable 10 Gbps Ethernet services for intra-providers (operators) or inter-providers.

VLAN translation/mapping, H-QoS dynamic bandwidth, and SLA management can be configured to enhance service.

In addition, digital diagnostics per the SFF-8472 standard can be performed for XFP transceivers of the OS930.

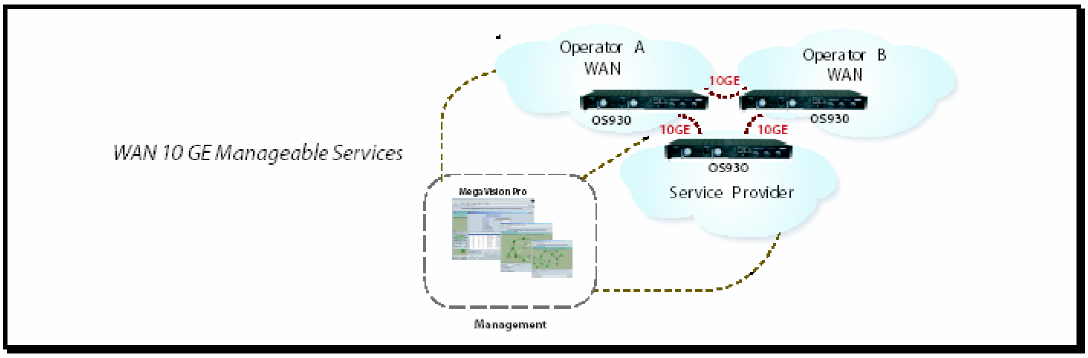



**Figure 7: WAN 10 Gbps Manageable Ethernet Services**

# 10 Gbps Ethernet Services over WDM

*Figure 8*, below, shows an application for placing 10 Gbps Ethernet services via XFPs on MRV's LambdaDriver WDM multiplexer that provides long-haul paths, fiber-optimization, and redundancy protection for services.

VLAN translation/mapping, H-QoS dynamic bandwidth, and SLA management can be configured to enhance service.

In addition, digital diagnostics per the SFF-8472 standard can be performed for SFP transceivers of the OS930. Layer 1 cable diagnostics (VCD) can be performed to identify and locate faults in copper cables/connections.

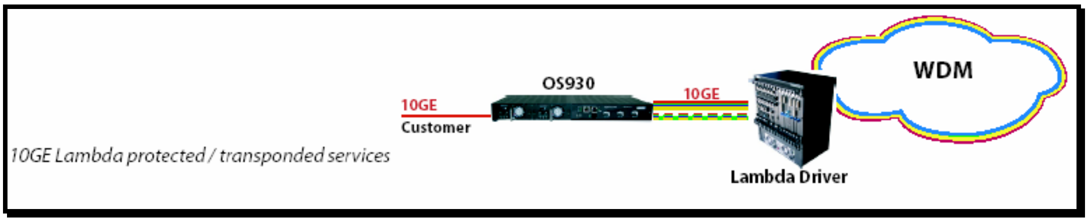



**Figure 8: 10 Gbps Ethernet Services over WDM**

# Chapter 3: Installation

## General

This chapter provides a detailed step-by-step procedure for installing the OS900.

## Safety

Before installing the OS900, ensure that the requirements noted in the section *Safety Requirements*, page *49*, are met.

## Package Contents

### Essentials

- OS900s (as many as ordered by the customer)
- EIA-232 Cable (1 per OS900)
- Power Cord (1 per power supply)
- CD containing the OS900 User Manual (1)

### Options

- Brackets for mounting the OS900 in a 19-inch or 23-inch rack (2 per OS900)
- WDM and/or E1/T1 CES and/or STM-1/OC3 modules (up to 2 per OS910-M)
- SFPs (up to 2 per OS904 or OS910-M)
- XFPs (up to 3 per OS930)
- A second power supply (1 per OS910-M or OS930
- *MegaVision Pro* ® server SNMP network management application (on CD)
- Outdoor Cabinet (1 for up to four OS900s)

## Requirements

### Tools

- Philips screwdriver no. 1
- Philips screwdriver no. 2

### Data Equipment

#### DTEs/DCEs

Compliant to IEEE 802.3, IEEE 802.3u, and/or IEEE 802.3z.

#### Cabling

***10/100/1000Base-T Ports***

*Cable Type*: Category 5.
*Cable Connector Type*: RJ45 8-pin male
*Cable Length*: Up to 100 m (330 ft)

*Cable Impedance*: 100 Ω

*Cable Wiring*: Straight (*Figure 78,* page *805*) or Cross (*Figure 79,* page *805*)

| | **Note** |
|---|---|
| | Each 10/100/1000Base-T port may be connected with a *straight-wired* or *cross-wired* cable irrespective of whether the co-port[6] is that of a DCE (e.g., switch) or DTE (e.g., PC) since the OS900 port automatically configures its interface to be Ethernet MDI or MDIX in order to communicate via the co-port. |

***100/1000Base-X Ports***

Cabling requirements are SFP dependent.

The cable length can be up to:

$$\frac{\text{[Output power of SFP transmitter} - \text{Sensitivity of SFP receiver] - Path losses (in dB)}}{\text{Cable Attenuation (in dB/km)}}\ km$$

The path losses must include losses due to interposing devices, splices, etc. plus a safety margin of 3 dB.

***10 GE Ports (Only in OS930)***

Cabling requirements are XFP dependent.

The cable length can be up to:

$$\frac{\text{[Output power of XFP transmitter} - \text{Sensitivity of XFP receiver] - Path losses (in dB)}}{\text{Cable Attenuation (in dB/km)}}\ km$$

The path losses must include losses due to interposing devices, splices, etc. plus a safety margin of 3 dB.

***WDM Module Ports (Only in OS910-M)***

For possible cabling configurations for WDM Module ports, refer to ***Chapter 37:*** *WDM Module*, page *623*.

***E1/T1 Module Ports (Only in OS910-M)***

Refer to ***Chapter 38:*** *E1/T1 CES Module*, section *Product Specification*, page *675*.

***STM-1/OC3 Module Ports (Only in OS910-M)***

Refer to ***Chapter 39:*** *STM-1/OC3 CES Module*, section *Product Specification*, page *707*.

***Cable Fiber Marking***

For *each* cable fiber, attach a label with the marking **Tx** at one end and another label with the marking **Rx** at the other end.

## Management Equipment

***Out-of-band* Management using Serial/RS-232 Connection**

- Craft terminal: Asynchronous ASCII terminal, e.g., *VT100* terminal
  ***or***
  Craft terminal emulator: For e.g., PC with asynchronous ASCII terminal emulation software application such as *Microsoft Wind, ows' HyperTerminal*
  ***or***
  UNIX workstation
  ***or***
  Linux workstation
- Operating System: For e.g., Microsoft Windows 95, 98, 2000, NT, or XP
- Cable (supplied by MRV): Null-modem RS-232, with RJ45 8-pin male connector and DB9 9-pin female connector, and ***not*** longer than 15 m

[6] A co-port is another port that receives from or forwards to the OS900 port.

(50 ft) for connecting the OS900 **CONSOLE EIA-232** port to the management station. The cable wiring is shown in *Figure 77* on page *805*.

***Out-of-band*** **Management using TELNET, SSH, or SNMP Connection**

- TELNET or SSH station: For e.g., PC with TELNET or SSH application
  ***or***
  SNMP NMS: For e.g., MRV's *MegaVision Pro®* network management application running on a PC. For details, refer to the *MegaVision User Manual*.
- Operating System: For e.g., Microsoft Windows 95, 98, 2000, NT, or XP.
- Interface to the Web: Optional, required for Web-Based Management.
- Cable: Category 5, with RJ45 male 8-pin connector, up to 100 m (330 ft) long for connecting the OS900 **MGT ETH** port to the network via which the management station can access the OS900. The cable must be cross-wired as shown in *Figure 79*, page *805*.
- IP Address: If an IP address is to be assigned to the OS900 for the first time, the interconnection described in the section *Craft Terminal/Emulator (For Out-of-band Management)*, page *81*, must be used.

## Mounting

Elevated Operating Ambient Temperature – If an OS900 is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient temperature. Accordingly, make sure that the operating ambient temperature of the rack environment is compatible with the maximum ambient temperature (Tma), 50 $^{o}$C (122 $^{o}$F).

Reduced Air Flow – Installation of the OS900 in a rack should be such that the amount of air flow required for safe operation of the OS900 is not compromised.

Mechanical Loading – Mounting of the equipment in the rack should be such that a hazardous condition is not developed due to uneven mechanical loading.

Ensure that the OS900 will be within reach of the necessary connections, namely, line/mains power outlet, Ethernet networks, and a craft terminal/emulator or a UNIX workstation if the OS900 is to be managed via its **CONSOLE EIA-232** port.

For mounting an OS900, any one of the following may be used: Rack, Wall, Outdoor Cabinet, or Desktop. Details are given below.

Rack:

– 19-inch rack:
  *One OS904, OS906/AC-1, OS906/DC-1, OS910/AC-1, or OS910/DC-1:*
  EM900-BR-1 bracket pair + four philips screws (supplied by MRV)
  *One OS910/AC-2 or OS910/DC-2*:
  EM304-BR-3 bracket pair + four philips screws (supplied by MRV)
  *One OS906/AC-2, OS906/DC-2, OS910-M, OS912-AC-2, OS912-DC-2, or OS930:*
  EM930-BR-1 bracket pair + four philips screws (supplied by MRV)
  *Two OS904s, OS906/AC-1s, OS906/DC-1s, OS910/AC-1s, or OS910/DC-1s (side-by-side)*
  EM900-BR-D Tray + spacer D + 10 philips screws (supplied by MRV)
  *One OS904, OS906/AC-1, OS906/DC-1, OS910/AC-1, or OS910/DC-1*, *and one LDP100 (side by side)*:
  EM900-BR-E Tray + spacer E + 11 philips screws (supplied by MRV)

– 23-inch rack:
  *One OS904, OS906/AC-1, OS906/DC-1, OS910/AC-1, or OS910/DC-*
  EM900-BR-2 bracket pair + four philips screws (supplied by MRV)
  *One OS910/AC-2 or OS910/DC-2*:
  EM304-BR-4 bracket pair + four philips screws (supplied by MRV)
  *One OS910-M, OS906/AC-2, OS912-AC-2, OS912-DC-2, or OS930:*
  EM910M-BR-2 bracket pair + four philips screws (supplied by MRV)

– Space in rack:

~ 220 x 45 x 240 mm $^3$
[~ 8. 5 x 1U x 9.5 in $^3$]

Wall:

- *One OS904, OS906/AC-1, OS906/DC-1, OS910/AC-1, or OS910/DC-1*:
  EM900-WBR bracket (supplied by MRV)

  The wall area must be at least:

  ~ 220 x 240 mm $^3$
  [~ 8. 5 x 9.5 in $^3$]

Outdoor Cabinet:

- Up to four OS900s indoors or outdoors (supplied by MRV)

Desktop:

- One per minimum surface area:

  ~ 220 x 240 mm $^3$
  [~ 8. 5 x 9.5 in $^3$]

  The surface must be flat, stable, non-conductive, and static-free.

## Environmental

*Temperature*: Per the OS900 model – refer to ***Appendix F:*** *Product Specification*, page *813*.

*Humidity*: Non-condensing, 10 to 85%.

*Cooling air*: Flowing around the OS900 and through the air vents unobstructed. In addition, there must be a clearance of at least 25 mm (1 inch) between the air vents and nearby objects.

## Power

The line (mains) should be able to supply power to the OS900 as specified on the nameplate of the OS900. Make sure there will be no overloading of supply circuits that could have an adverse effect on overcurrent protection and supply wiring.

### AC Source

The AC power source (line/mains) should be able to supply power to the OS900 according to the section **Power Consumption (Max)**, on page *816*.

The power cord for 115 Vac input from a power source must be a minimum-type SJT (SVT) 18/3, rated 250 Vac, 10 A with a maximum length of 4.5 m or 15 ft. One end must terminate in an IEC 320 attachment plug, the other end must terminate in a NEMA 5-15P plug.
(The power cord supplied by MRV meets these requirements.)

The power cord for 230 Vac input from a power source must be a minimum-type SJT (SVT) 18/3, rated 250 Vac, 10 A with a maximum length of 4.5 m or 15 ft. One end must terminate in an IEC 320 attachment plug, the other end must terminate as required by the recognized safety organization of the country in which it is installed.

### DC Source

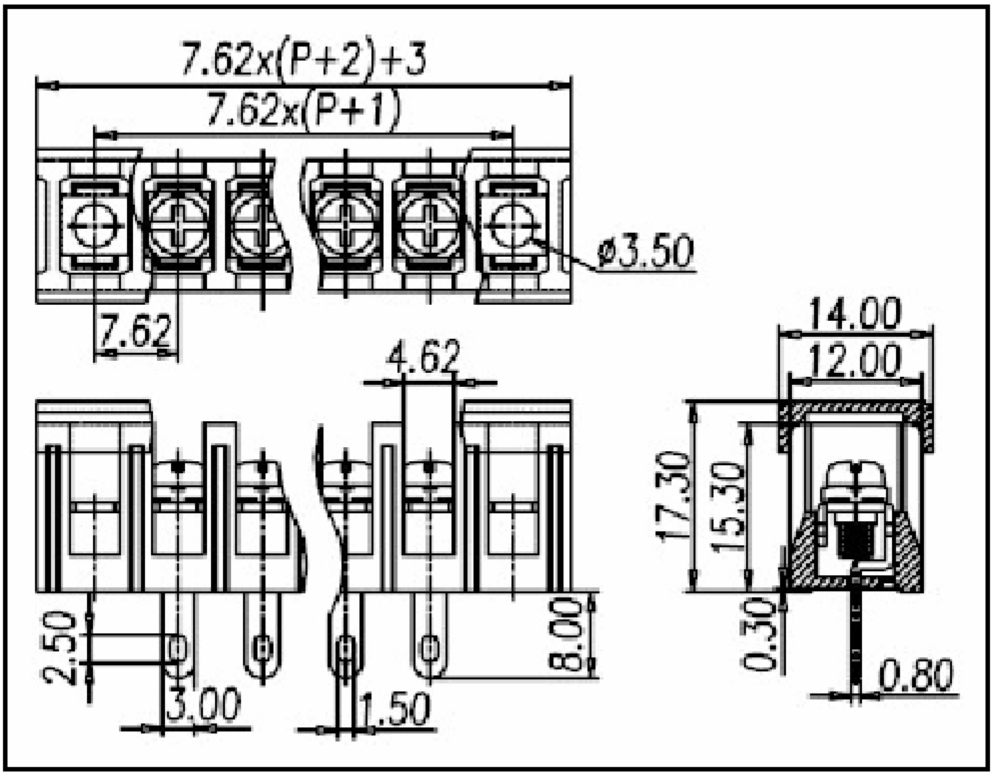
The DC power source should be able to supply power to the OS900 according to the section **Power Consumption (Max)**, on page *816*.

DC rated equipment must be installed in the following conditions:

1. The DC supply source to which the OS900 is to be connected must be isolated from the alternating current source and reliably connected to earth or to a DC (SELV) source.
2. The OS900 must be installed only in restricted access areas (Dedicated Equipment Rooms, Equipment Closets, or the like) in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
3. Input wiring to a terminal block must be routed and secured in such a manner that it is protected from damage and stress. Do not route wiring past sharp edges or moving parts.
4. A readily accessible disconnect device, with a 3 mm minimum contact gap shall be incorporated in the fixed wiring.

5. A listed circuit breaker suitable for protection of the branch circuit wiring and rated 60 Vdc minimum must be provided.
6. The following specifications of the DC power block are to be taken into consideration for preparing/connecting a DC power cable: *Rated voltage*: 300 V; *Rated current*: 15 A; *Plastic housing*: PBT/UL94V-0/Black; *Terminal*: Brass/0.8t/tin-plated; *Screw*: Steel/M3/nickel plated.

   The DC power cable must be #18 AWG with soldered ends. Connector lugs are not essential. The DC power cable *connector* must match the measurements of the DC power block as shown below.




   MRV's CAB3-18T DC power cable is suitable for connection to the DC power block. It has the following specifications: 3m long, #18 AWG, fitted with connector lugs, terminated at one end. The terminated end of the cable is to be connected to the DC power supply connector.

**Power Supplies**

One power supply may be sufficient for the OS900.

A second power supply ensures continued supply of requisite power even if a power supply fails.

In models OS910-M and OS930, the positions and functions of a power supply's switch  are as follows:

I Position: Allows power from the AC line (mains) into the OS900

O Position: Prevents power into the OS900.

**UPS**

To ensure continued operation even when the line (mains) power is cut off, it is recommended to connect the OS900 through a UPS.

## Grounding

Reliable earthing of the OS900 must be maintained. Particular attention should be paid to supply connections when connecting to power strips rather than to direct connections to the branch circuit. The butterfly nut on screw for earthing is of type NC6.

# Procedure

## Component Insertion

#### SFP/XFP

1. Choose the SFP/XFP receptacle into which the SFP/XFP is to be inserted.
2. Holding the SFP/XFP with the right side up, slide it about half-way into the SFP/XFP receptacle.
3. If the SFP/XFP has a latching mechanism, while holding the SFP/XFP with one hand gently release the latch with the other hand. Usually, the latch handle is a wire frame around the SFP/XFP. To release the latch, swing down the wire frame.
4. With both thumbs pressed against the face edges of the SFP/XFP, gently slide it as far into the SFP/XFP receptacle as possible. Holding the SFP/XFP in this position, swing up the latch handle around the SFP/XFP in order to latch it.

#### WDM Module (Only in OS910-M)

Refer to ***Chapter 37:*** *WDM Module*, section *Mounting*, page *624*.

#### E1/T1 CES Module (Only in OS910-M)

Refer to ***Chapter 38:*** *E1/T1 CES Module*, section *Mounting*, page *632*.

#### STM-1/OC3 Module (Only in OS910-M)

Refer to ***Chapter 39:*** *STM-1/OC3 CES Module*, section *Mounting*, page *681*.

#### Power Supply Module, e.g., EM9-M-PS (Only in OS910-M and OS930)

1. Choose the receptacle in the OS900 into which the power supply module is to be inserted.
2. Holding the power supply module with the right side up, place the edges of the module's PCB between the left and right rails in the receptacle and slide it until its panel is level with the front panel of the OS900. (This assures that the module's connector is inserted into place.)
3. With a philips screwdriver no. 1, fasten the module with the two captive screws that are located on its edges.

## Mounting

#### Rack

#### *19-inch*

<u>One OS900</u>

1. With four screws, fasten the two mounting brackets[7] to the sides of the OS900 as shown in *Figure 9*, below.
2. Mount the OS900 in a 19-inch rack.

**Figure 9: *19-inch* Brackets Fastening for Mounting one OS900 in a Rack**

[7] Either bracket may be mounted on either side.

Two OS900s Side-by-Side (Only OS904s, *OS906/AC-1s, OS906/DC-1s,* OS910/AC-1s, and OS910/DC-1s)

1. With four screws, fasten one OS900 on the left side of the tray as shown in *Figure 10*, below.
2. With two screws, fasten the spacer to the right side of the OS900.
3. With four screws, fasten the second OS900 on the right side of the tray as shown in *Figure 10*, below.
4. Mount the tray in a 19-inch rack.

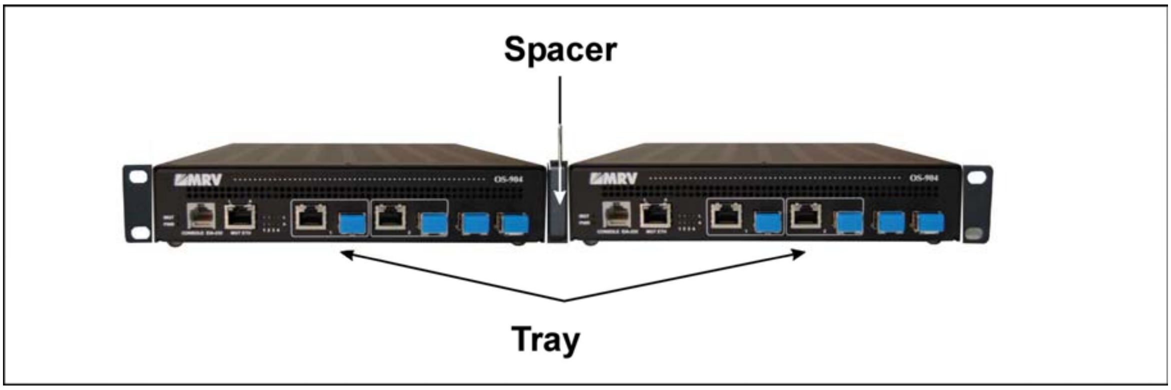



**Figure 10: 19-inch Tray Fastening for Mounting two OS900s in a Rack**

One OS900 and One LDP100 (Only OS904, *OS906/AC-1, OS906/DC-1,* OS910/AC-1, or OS910/DC-1)

1. With four screws, fasten the OS900 on the left side of the tray as shown in *Figure 11*, below.
2. With two screws, fasten the spacer to the right side of the OS900. With one screw, fasten the spacer to the tray.
3. With four screws, fasten the LDP100 on the right side of the tray as shown in *Figure 11*, below.
4. Mount the tray in a 19-inch rack.

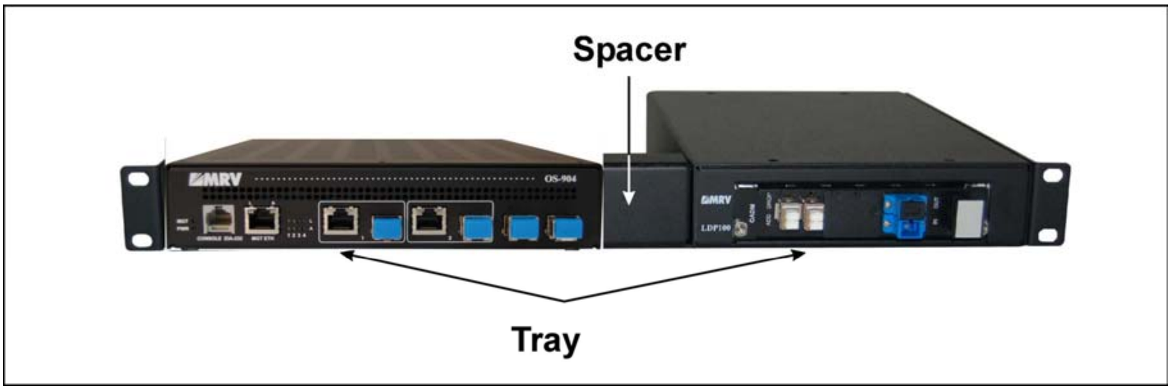



**Figure 11: 19-inch Tray Fastening for Mounting one OS900 + one LDP100 in a Rack**

***23-inch***

1. With four screws, fasten the two mounting brackets[8] to the sides of the OS900 as shown in *Figure 12*, below.
2. Mount the OS900 in a 23-inch rack.

[8] Either bracket may be mounted on either side.

**Figure 12: *23-inch* Brackets Fastening for Mounting one OS900 in a Rack**

**Wall (Only OS904, OS906/AC-1, OS906/DC-1, OS910/AC-1, and OS910/DC-1)**

Fasten the wall bracket by inserting two flat-head philips screws (no longer than 3 mm) at two holes (having counter sinks) on the underside of the OS900 as shown in *Figure 13*. Fix two wall screws 100 mm (4 inch) apart and hang the OS900.


**Figure 13: Wall Bracket Fastening to an OS900**

**Outdoor Cabinet**

Refer to the *Outdoor Cabinets User Manual*, *Publication No. ML46852*.

**Desktop**

Place the OS900 on a flat, stable, non-conductive static-free surface.

## Earthing

With an insulated copper wire of gage up to #18 AWG, connect the OS900 to an earthing point at its butterfly-nut-on-screw located at the rear.

## Network Connection

### Service Modules

***WDM Ports***

Refer to the section *Network Connection*, page *624*.

***E1/T1 Ports***

Refer to the section *Cabling* page *632*.

***STM-1/OC3 Ports***

Refer to the section *Cabling* page *681*.

### Data Equipment (DTE or DCE)

Connect the data ports[9] of the OS900 to the data equipment with cables as follows:

***Electrical Ports***

Use a straight-wired or cross-wired cable (specified in the section *10/100/1000Base-T Ports*, page *73*) to connect each OS900 electrical data port to a DTE or DCE.

[9] Data ports are also referred to as LAN/WAN or customer ports

#### *Fiberoptic Ports*

Using fiberoptic cables connect each optical data port of the OS900 to a DTE or DCE making sure that:

A port on one device is to be connected to a port on another device as follows: The end marked **Tx**[10] of one fiber of a cable is connected to the Tx port of a (first) device and the end marked **Rx** to an Rx port of another (second) device. For the *other* fiber of the cable, the end marked **Rx** is connected to an Rx port of the first device and the end marked **Tx** to a Tx port of the second device.

### Management Station

Connect at least one of the following to the OS900: Craft terminal, TELNET station, SSH station, UNIX station, Linux station, or SNMP NMS, as described below.

#### *Craft Terminal/Emulator (For Out-of-band Management)*

With a null-modem RS-232 cable having an RJ45 8-pin *male* connector, connect the OS900's RJ45 8-pin female connector marked **EIA-232** to a craft terminal/emulator serial port.

#### *TELNET/SSH Station or SNMP NMS*

Connect the OS900 to a TELNET, SSH, or SNMP station in *either* of the following ways:

– With a Category 5 cable (straight-wired or cross-wired) having an RJ45 8-pin *male* connector, at the dedicated out-of-band management port marked **MGT ETH** or at a 10/100/1000Base-T port.

– With a fiberoptic cable, at a 100/1000Base-X SFP port.

## Power Source Connection

### AC Source

1. Make sure that the power cord (supplied) for the OS900 is ***disconnected*** from the power source (line/mains).
2. The following substeps apply to OS900 models with a 'Power Cord Fastener,' shown in the picture of the ***Rear*** of the OS904, page *60*. They are to be performed in order prevent unintentional disconnection of the power cord.
   2.1. Plug one end of the power cord into the 'AC Power Receptacle'.
   2.2. Remove the philips screw located on the 'Power Cord Fastener'.
   2.3. Lift up the free end of the 'Power Cord Fastener'.
   2.4. Place the power cord under the free end of the 'Power Cord Fastener' and against the side of the OS900.
   2.5. Bring down the free end of the 'Power Cord Fastener' over the power cord.
   2.6. Using the philips screw (removed in Step *2.2*, above), fasten the power cord to the side of the OS900.
3. Connect the other end of the power cord to the power source (line/mains).

### DC Source

1. Make sure that the power cable for the OS900 is ***disconnected*** from the power source.
2. Connect the terminated end of the cable to the DC power supply connector on the OS900 as follows: White wire → **+** ; Black wire → **–** ; Green wire → ⏚.
3. Connect the other end of the power cable to the DC power source.

[10] Marking of the fibers is described in the section *Cable Fiber Marking*, page *74*.

# Chapter 4: Startup, Setup, and Operation

## Startup

To start up the OS900, connect it with its power cord(s) to the power source (line/mains), and, if it is an OS910-M or OS930 set each power supply switch ( ) to the ON ( ) position.

This causes the OS900 to undergo a sequence of operationality and initialization tests. At the end of the tests, which last a few seconds, the OS900 becomes fully operational as a basic switch that can perform Layer 2 switching between its ports.

## Setup

### Operation

#### Default

The default setup is a collection of settings assumed by the OS900 when settings are not assigned by the administrator. Each default setting can be changed by invoking its associated CLI command, described in the relevant parts of the manual. The section *Invoking a CLI Command*, page *94*, shows how to invoke CLI commands.

If the factory default settings are changed, they can be restored as described in the section *Restoration of Factory Default Configuration*, page *521*.

#### Custom

A setup can be changed using any of the management stations described in the section *Management Equipment*, page *74*. The connection of management stations is described in the section *Management Station*, page *81.* The required setup of the craft terminal is described in the section *Local Management (Craft Terminal)*, page *83*.

Unlike the RS-232 interface, the Ethernet interface (**MGT ETH** port) or a VLAN interface has to be enabled for management in order to perform setup. The procedure for enabling management via these interfaces is given in the section *Remote Management*, page *191*.

Additional setup using the OS900's CLI is required to activate specific functions of the OS900. (Examples of such functions are: VLANs, Provider bridges, Traffic policing, and Link aggregation.)

Use of the CLI is described in ***Chapter 5:*** *CLI Management*, page *87*. The available functions and their activation are described in their respective sections/chapters.

### Management

#### Local Management (Craft Terminal)

Make sure that a connection exists between the management station and the OS900 **EIA-232** port. The interconnection is shown in the section *Craft Terminal/Emulator (For Out-of-band Management)*, page *81*.

If you are using a PC, run the emulation software application (e.g., Microsoft Window's HyperTerminal or TeraTermPro), and set up the craft terminal/emulator as shown in *Table 4*, below.

**Table 4: ASCII Craft Terminal/Emulator Setup for CLI Management**

| Transmit/Receive Rate (Baud) | Data Length (Bits) | Parity | Stop Bits | Flow Control |
|---|---|---|---|---|
| 9600 | 8 | None | 1 | None |

**Remote Management (TELNET/SSH/SNMP)**

For remote management setup, familiarity is required with the CLI and with interface configuration. Accordingly, setup details are given in the section *Remote Management*, page *191*.

# Operation

## Monitoring

The OS900 becomes fully operational within a few seconds after being powered ON. Its operation can be monitored by interpreting the status of its LEDs with the aid of *Table 5*, below, or with a management station (e.g., craft terminal, TELNET, UNIX, or Linux station, SSH host, or SNMP NMS).

**Table 5: Front Panel LEDs**

| Level | LED | Status | Significance |
|---|---|---|---|
| Global | **PWR** (Power) | ON-Green | Power *into* the OS900 system *OK*. |
| | | ON-Amber | Power present at the entrance to but not in the OS900 system. (In OS900 models other than OS910-M, when pushbutton **PWR** is pressed continuously for *at least* 2 seconds, LED **RST** turns ON-Green. When power to the OS900 system is shutdown, LED **PWR** turns ON-Amber.) |
| | | OFF | *No* power at the entrance to the OS900 system. |
| | **PS1** (Power Supply 1) | ON-Green | Power distribution to OS900 system from Power Supply 1 *OK*. That is, power cord connecting Power Supply 1 to line/mains, and (in OS910-M and OS930) Power Supply 1 switch in position I (power ON). |
| | | OFF | Power distribution to OS900 system from Power Supply 1 *faulty*. That is, power cord disconnected or (in OS910-M and OS930) Power Supply 1 switch in position O (power OFF). |
| | **PS2** (Power Supply 2) | ON-Green | Power distribution to OS900 system from Power Supply 2 *OK*. That is, power cord connecting Power Supply 2 to line/mains, and (in OS910-M and OS930) Power Supply 2 switch in position I (power ON). |
| | | OFF | Power distribution to OS900 system from Power Supply 2 *faulty*. That is, power cord disconnected or (in OS910-M and OS930) Power Supply 2 switch in position O (power OFF). |
| | **RST** or **PRP** (Reset) | ON-Green | In OS900 models other than OS910-M, while the OS900 was powered ON, *either* pushbutton **RST** *or* pushbutton **PWR** was pressed continuously for *at least* 2 seconds. |
| | | OFF | Normal operation. |
| | **TMP** or **TEMP** (Temperature) | ON-Green | Internal temperature of operating OS900 system *OK*. |
| | | ON-Amber | Internal temperature of operating OS900 system *too high*. (The internal temperature can be displayed by invoking the CLI command `show version`.) |
| | **FAN** (Fan) | ON-Green | OS900 system internal fans *OK*. |
| | | ON-Amber | One or more OS900 system internal fans *faulty*. |
| | | OFF | No power into the OS900 system. |
| | **MGT** (Management) | ON-Green | Management traffic flowing to/from CPU. |
| | | OFF | *No* management traffic flowing to/from CPU. |

**Table 5: Front Panel LEDs** (Cont'd)

| Level | LED | Status | Significance |
|---|---|---|---|
| Per Port | **L&A** (Link and Activity) | ON | Port link integrity to network *OK*, port ***not*** receiving or transmitting data. |
| | | BLINKING | Port link integrity to network *OK*, port receiving or transmitting data. |
| | | Amber | Port speed 10/100 Mbps. |
| | | Green | Port speed 1000 Mbps. |
| | | OFF | Port link integrity to network broken or *faulty*. |
| | **L** (Link) | ON-Green | Port link integrity to network *OK*. (Only for *SFP* interface type.) |
| | | ON-Amber | Port link integrity to network *OK*. (Only for *10/100/1000-T fixed* interface type.) |
| | | OFF | Port link integrity to network broken or *faulty*. |
| | **A** (Activity) | ON-Green | Port receiving or transmitting data. |
| | | OFF | Port neither receiving nor transmitting data. |

## Reset

The reset function is used to restart the OS900 system without powering it OFF and ON.
To reset the OS900, press pin pushbutton **RST**.

## Shutdown

In OS904, OS906, OS910, and OS912

To shut down system operation, simply disconnect the power cord(s) from the power source (line/mains).

In OS910-M and OS930

To shut down system operation, set the switch  of each power supply to the OFF () position.

# Chapter 5: CLI Management

## General

This chapter describes the following:

– Command Line Interpreter (CLI) management tools
– Generic custom setup/management of the OS900 using CLI commands.

A CLI command may be a factory CLI command or a user-configured script. Scripts are given in the section *Scripts*, page *118*.

For custom setup/management to operate with specific protocols (e.g., MSTP) and utilities (e.g., DNS) refer to the relevant chapters.

The OS900 is shipped out of the factory already set up. The setup is only partial and allows basic Layer 2 switching between the Ethernet ports. However, additional settings may be required such as, for example, an IP address for the OS900.

For SNMP management using a PC running MRV's Network Management application, refer to the *MegaVision® Network Management User Manual*.

## CLI Access

### General

The CLI can be accessed via a Serial/RS-232, TELNET, SSH, or SNMP connection even while the OS900 is under normal operation.

### Access Levels

The OS900 has four CLI access levels, each appropriate to the expertise and authority of the user. The user enters a level with the password associated with the level. The access levels are as follows.

- **Admin Level:** At this level, only general display and external connectivity commands can be accessed. These commands can be used to display system version, check connectivity with another system, logout, etc. To enter this level, after the system is initialized, enter the login username and password.
- **Enable Level:** At this level, Admin Level and general system commands can be accessed. These commands can be used to monitor system operation, upgrade software, reboot the system, etc. To enter this level, after login at Admin Level, invoke the CLI command **`enable`**, followed by an additional password if set by the administrator.
- **Configure Level:** At this level, all system operation configuration commands can be accessed. To enter this level, after login at Enable Level, invoke the CLI command **`configure terminal`**, followed by an additional password if set by the administrator.
- **Root Level:** At this level, the OS900 operating system, Linux, can be accessed. To enter root level, after login at Enable Level, invoke the command **`linux`**. To become a root user (superuser), enter the command **`su`** followed by the root password. Details are given in the section *Linux Mode*, page *101*.

The procedure for configuring the *root* level and *admin* level passwords are given in the section *First Time Access – Root and Admin Passwords Configuration*, page *88*.

The procedure for configuring the *enable* level password is given in the section *Configuring/Changing the Enable Password*, page *103*.

The procedure for configuring the *configure* level password is given in the section *Configuring/Changing the Configure Password*, page *104*.

## Preparation

The following information is a prerequisite for configuring the OS900:

- A map of your network topology
- A list of VLANs to be configured on ports
- The IP addressing plan for each network interface
- The protocols required by the network
- The protocols to be used
- Location and IP address of each remote management station

## First Time Access – Root and Admin Passwords Configuration

Passwords are encrypted to provide added security against unauthorized access and configuration changes. A password can contain numerical characters (e.g., **1**, **2**, **3**, etc.), symbols (e.g., **$**, **%**, **@**, etc.), hyphens (-), uppercase letters (**A**, **B**, **C**), and lowercase letters (e.g., **a**, **b**, **c**, etc.).

When accessing the OS900 CLI for the first time, both the *root* (superuser-level) password and the *admin* (administrator-level) password should be configured.

> **Note**
> If the *root* or *admin* password is not configured, the OS900 can be accessed simply by pressing Enter in response to the system prompt to enter the password!

The *root* password is for accessing the OS900 Operating System (Linux) in order to change its operating *functions*. The *admin* password is for accessing the OS900 CLI in order to configure operation of the OS900.

The procedure for configuring *root* and *admin* passwords is as follows:

1. Power up the OS900.
2. When the prompt:
   ```
   MRV OptiSwitch 904 version 1_3_1
   OS900 login:
   ```
   appears, type **root** and press Enter.
3. When the prompt:
   ```
   You are required to change your password immediately (root enforced)
   Enter new UNIX password:
   ```
   appears, type a *root* password that is six or more characters long and press Enter.
4. When the prompt:
   ```
   Retype new UNIX password:
   ```
   appears, retype the root password and press Enter.
5. Type **exit** and press Enter.
6. When the prompt:
   ```
   logout
   MRV OptiSwitch 904 version 1_3_1
   OS900 login:
   ```
   appears, type **admin** and press Enter.
7. When the prompt:
   ```
   You are required to change your password immediately (root enforced)
   Enter new UNIX password:
   ```

appears, type an *admin* password that is six or more characters long and press Enter.

8. When the prompt:

```
Retype new UNIX password:
```

appears, retype the admin password and press Enter.

The system responds with:

```
Last login: Wed Jul 13 09:51:59 2007 on ttyS0
OS900>
```

indicating that CLI is ready for access.

In order to store these passwords in flash (permanent) memory, invoke the command **`write file`** or **`write memory`**. The passwords can be changed as described in the section *Passwords*, page *102*.

Below is an example showing configuration of the *root* and *admin* passwords. The strings of asterisks shown as user passwords are only representations of the passwords; the passwords (including their length) are actually hidden from view during entry.

```
MRV OptiSwitch 904 version 1_3_1
OS900 login: root
You are required to change your password immediately (root enforced)
Enter new UNIX password: ******
Retype new UNIX password: ******
# exit
logout
MRV OptiSwitch 904 version d0920-03-07-07
OS900 login: admin
You are required to change your password immediately (root enforced)
Enter new UNIX password: ******
Retype new UNIX password: ******
Last login: Wed Jul 13 09:51:59 2007 on ttyS0
OS900> write file
OS900>
```

## Standard Access

To access the OS900 for regular management (e.g., monitoring the network, changing system operation configuration, upgrading software, saving configurations, etc.), i.e., excluding access to the Linux operating system:

1. Power up the OS900. After initialization is completed (in about one minute), the following prompt will appear:

```
MRV OptiSwitch 910 version 1_3_1
OS900 login:
```

2. Enter the login name **`admin`**. The following prompt will appear:

```
Password:
```

3. Type in the admin password (configured as described in the section *First Time Access – Root and Admin Passwords Configuration*, page *88*). If no admin password was configured, the default is no password. In such case, simply press Enter.

The system prompt [11] (e.g., `OS910>`) will appear to indicate that connection to the CLI is established and the OS900 is ready for *local* management. For *remote* management, the OS900 must first be enabled as described in the section *Remote Management*, page *191*.

[11] The default system prompt identifies the model of the OS900.

# CLI Modes

A CLI mode (or node) is a stage at which a specific group of CLI commands is available to the administrator for interacting with the OS900. To enter a mode, type its name and press Enter. The system prompt includes the mode name to signify entry into the mode.

A mode itself may contain other modes (in addition to commands). On accessing the CLI (as described in the section *CLI Access*, page *87*), the modes (and commands) in each mode can be displayed by pressing Shift ?.

# Viewing CLI Commands

On accessing the CLI (as described in the section *CLI Access*, page *87*), the commands in a mode together with their description can be *viewed* as follows:

1. Type the name of the mode containing the CLI command to be viewed.
2. Press Shift ?.

# Conventions for CLI Commands

*Table 6*, below, describes the conventions used for CLI commands as presented in this manual.

**Table 6: Conventions for CLI Commands**

| Convention | Description |
|---|---|
| **`Courier Bold`** | This typeface represents information provided ***to*** the system. The information may include an argument, i.e, part of a CLI command. |
| `Courier` | This typeface represents information provided ***by*** the system. |

# Symbols in CLI Commands

*Table 7*, below, describes the symbols used in CLI commands.

**Table 7: Symbols in CLI Commands**

| Symbol | Significance |
|---|---|
| **`argument in lower case (keyword)`** | Argument to be entered as is. |
| **`ARGUMENT IN UPPER CASE (VALUEWORD)`** | Argument to be replaced with a value.<br>To specify number values:<br>Type the individual numbers separated by commas<br>and/or<br>Type the lowest and highest number separated by a hyphen (**-**) to specify a range of consecutive numbers.<br>Example: To specify numbers 1, 3, 4 to 7, and 9, type **`1,3,4-7,9`** |
| **`[ ]`** | Optional command argument enclosure.<br>Do *not* type this symbol with the command argument! |
| **`(CR)`** | Typed command (whatever it is) can be invoked by pressing Enter. |
| \| | Process the output of a CLI command by any Linux command (e.g., **`wc`**, **`grep`**, **`tail`**, etc.). |
| `OS900>` | prompt of **`disable`** mode. |
| `OS900#` | prompt of **`enable`** mode. |
| `OS900(config)#` | prompt of **`configure terminal`** mode. |

# Functional Keys for CLI Commands

**Table 8: Functional Keys for CLI Commands**

| Key | Function |
|---|---|
| Tab | Used to complete a keyword after its first few characters are typed. Tab adds characters to a partially typed keyword to form a character string that is common to all keywords beginning with the partially typed keyword. If the partially typed keyword is unique to a keyword, Tab completes the keyword. If the partially typed keyword is not unique to a keyword, additional characters will have to be typed in order for Tab to complete the keyword. |
| Enter | *After the first few characters of a command are typed:*<br>Executes the command if these characters are a complete command or even if they are unique to the command.<br>Displays the message<br>`% Command incomplete`<br>if the characters are not a complete command.<br>Displays the message<br>`% Unknown command`<br>if the first characters are not those of any command.<br>*When the prompt* `--More--` *appears*<br>Displays the next line in the list if a show command was invoked.<br>Displays the next batch of lines in the list if ? was pressed immediately after a mode indication (e.g., `OS9024-4C(config)#`.) |
| ? | *After the system prompt:*<br>Displays all the modes/commands selectable at the current CLI level.<br>*After the first few characters are typed:*<br>Displays selectable modes/commands/arguments beginning with these characters.<br>*After a word (mode, command, or argument) is typed:*<br>Displays a set of arguments from which one is selectable. |
| Spacebar | Scrolls displayed list. |
| Q | Changes access to the higher mode. |
| Ctrl A | Moves the cursor to the first character on the line. |
| Ctrl B or ← | Moves the cursor back one character. |
| Ctrl F or → | Moves the cursor forward one character. |
| Ctrl E | Moves the cursor to the end of the current command line. |
| Del or Backspace | Deletes the character to the left of the cursor. |
| Ctrl W | Deletes the last word typed. |
| Ctrl U or Ctrl X | Deletes all characters from the cursor position to the *beginning* of the command line. |

**Table 8: Functional Keys for CLI Commands** (Cont'd)

| Key | Function |
|---|---|
| Ctrl K | Deletes all characters from the cursor position to the *end* of the command line. |
| Ctrl L or Ctrl R | Repeats the current command on a new line. |
| Ctrl Z or Ctrl C | Returns to enable mode from any other mode. |
| ↑ | Displays *earlier* invoked commands. |
| ↓ | Displays *later* invoked commands. |

# Help

By pressing Shift ? when the cursor is in differing positions in a command, different information on the command/argument can be obtained.

**Note**

**?** does not appear in the CLI display when Shift ? is pressed. However, it is shown in the following example (and elsewhere) for clarity.

- **CLI Help:** Press Shift ? at the system prompt of any mode to see the commands available in that mode. The following example shows the commands available in **disable** mode when you press Shift ? in **disable** mode.

```
OS900> ?
  enable       Turn on privileged mode command
  exit         Exit current mode and down to previous mode
  help         Description of the interactive help system
  list         Print command list
  logout       Logout from this current session
  monitor      Monitor
  nslookup     Name server query
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  show         Show running system information
  telnet       Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
OS900>
```

- **Partial Keyword Help:** To view the list of commands that begin with a partial keyword you have typed, without inserting a space after the last character of the partial keyword, press Shift ?. For example, when you type **de** and press Shift ?, the following results are displayed:

```
OS900(config)# de?
  debug        Debugging functions (see also 'undebug')
  default      Negate a command or set its defaults
  default-fwd  Set default forwarding
OS900(config)# de
```

- **Keyword Definition Help:** To view the definition of a command or keyword that you have typed, without inserting a space after the last character of the keyword, press Shift ?. For example, when you type the command **port** and press Shift ?, the following results are displayed:

```
OS900(config)# port?
  port  Port configuration
```

```
OS900(config)# port
```

- **Command Syntax Help:** To view a list of valid keywords and arguments for a command you have typed, insert a space after the last character of the command and press Shift ?. This list contains all the relevant commands, keywords, and arguments relating to the command you have typed. For example, when you type **`port`** and press Shift ?, the following results are displayed:

```
OS900(config)# port ?
  core-ethertype-1      Set ethertype-1 mode
  core-ethertype-2      Set ethertype-2 mode
  access-group          Enable access lists on port
  acl-binding-mode      Set port acl binding mode
  advertise             Advertise default auto-negotiation capabilities
  buffers               Buffers setting
  default               Set port speed and duplex to default value
  description           Set port description
  duplex                Port duplex mode
  egress-shaping        Egress rate shaping
  errdisable            Disable port when a preconfigured cause is detected
  flood-limiting        Limit type
  flow-control          Port flow control mode
  ingress-shaping       Ingress rate shaping
  l2protocol-tunnel     Layer 2 protocol tunneling specification
  lacp                  Port lacp mode
  lt-learning           Enable port lt learning
  media-select          Select media for the port
  mirror                Mirroring packets received to the analyzer
  mtu-size              Configure Maximum Transmit Unit size
  priority-queuing      Bind port to scheduling profile
  protected             Egress protected
  qos-marking           Set QoS marking mode
  qos-trust             Set QoS trust mode
  rapid-lacp            Port rapid lacp mode
  redundancy            Set redundancy mode for APS port
  shaper                shaper mtu size configuration
  sl                    Port service-level
  sl-account            Service level port accounting
  speed                 Port speed configuration
  state                 Port state
  tag-outbound-mode     Set port outbound tag mode
  trunk                 Create a port trunk entry
  udld                  Uni-Directional Link Detection protocol
  untagged-multi-vlans  Set port to untagged with multi vlans
OS900(config)# port
```

# Listing CLI Commands

To display the list of all CLI commands in all valid syntaxes that are available at any mode:

1. Enter the mode.
2. Invoke the command **`list`**.

The CLI commands are displayed in alphabetical order as shown in the example below.

```
OS912C(config-line)# list
  alias (all|this|NODENAME) NAME ...
  end
  exec-timeout current-session <1-35791>
  exec-timeout current-session default
  exec-timeout global <1-35791>
  exec-timeout global default
  exit
  help
  list
  max-open-vtysh <1-10>
  no alias (all|this|NODENAME) NAME
  no alias (all|this|NODENAME) NAME ...
  no exec-timeout current-session
  no exec-timeout global
  quit
  show alias
  show alias (all|this|NODENAME) [NAME]
  show history
  show line vty configuration
  show max-open-vtysh
  write file
  write file NAME
  write memory
  write terminal
OS912C(config-line)#
```

# Invoking a CLI Command

## General

A CLI command consists of a name and none, one, or several arguments. The name may be one word (e.g., **`interface`**) or hyphenated words (e.g., **`radius-server`**). An argument must be preceded by a blank space. It may be a *keyword* (identified by *lower*case text) or a *valueword* (identified by *upper*case text). If a keyword is selected, it must be typed in as is. If a *valueword* is selected, a value must be typed instead of it. The value may be just a number or a string consisting of letters, number digits, and other symbols. Valid values are either displayed or can be determined from the description of the *valueword*.

## Procedure

To invoke a CLI command:

1. Enter the mode containing the command.
2. Type the command name.
   (If you are not sure of the full name of the command, type its first few letters and press Shift ?. Command names beginning with these letters are displayed. Identify the command name you need, and type in one or more additional letters of the command name until the letters are now unique to the command. To complete the command name, press Tab.)
3. Press Shift ? to display arguments (if any) that need to be entered. Identify the argument you need. If the argument is a keyword (identified by *lower*case text), type the first few letters that are unique to the argument and press Tab. If the argument is a valueword, type a value for it using the description given for the value as a guide.
4. Repeat Step *3*, until the symbols `(CR)` and `|` appear.
5. Press Enter to invoke the command.

## Example

The following example illustrates how a CLI command can be invoked. The procedure is described in considerable detail to serve as a guide for invoking other CLI commands and to show how various functional keys can be used when invoking a CLI command. These functional keys help in producing the command in its correct syntax while minimizing typing.

Suppose the aim is to invoke the command **`interface vlan IFNAME`**. Access the CLI (as described in the section *Standard Access*, page *89*). When the system prompt (e.g., `OS900>`) is displayed, press Shift ? to display the commands available at this level. The CLI response is shown below.

```
OS900> ?
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  help        Description of the interactive help system
  list        Print command list
  logout      Logout from this current session
  monitor     Monitor
  nslookup    Name server query
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
OS900>
```

Notice that the symbol '`?`' does not actually appear on the screen. Still, it is shown to indicate that Shift ? was pressed after the CLI prompt '`OS900>`'.

Also, notice that a description appears against each command.

Type '**`e`**' and press Shift ?. The CLI response is shown below.

```
OS900> e?
  enable  Turn on privileged mode command
  exit    Exit current mode and down to previous mode
OS900> e
```

Notice that the two commands **`enable`** and **`exit`** are displayed because both these commands begin with **`e`**. To select the command **`enable`** type '**`n`**' (after the '`e`' to get '`en`,' which is different from 'ex' in the command **`exit`**), and press Tab. Then press Enter. The CLI response is shown below.

```
OS900> enable
OS900#
```

Notice that the system prompt has changed from '`OS900>`' to '`OS900#`'.

'`#`'indicates entry into **`enable`** mode.

Next, type '**`con`**' and press Tab. The CLI response is shown below.

```
OS900# configure
```

Press Shift ? to determine possible argument choices. The CLI response is shown below.

```
OS900# configure ?
  <cr>
  terminal  Configuration terminal
  |         Output modifiers
OS900# configure
```

Type '**`t`**' for '`terminal`', press Tab, and then press Shift ?. The CLI response is shown below.

```
OS900# configure terminal
  <cr>
  |     Output modifiers
OS900# configure terminal
```

Notice that only the symbols '`<cr>`' and '`|`' appear. This indicates that the command **`configure terminal`** can now be invoked.

Invoke the command **`configure terminal`** by pressing Enter. The CLI response is shown below.

```
OS900(config)#
```

Notice that the system prompt has changed from '`OS900#`' to '`OS900(config)#`'.
You now have access to **`configure terminal`** mode.

You can now press Shift ? to determine possible command choices in the mode.

Type '**`i`**' and press Shift ?. The CLI response is shown below.

```
OS900(config)# i?
  igmp                IGMP specific commands
  ingress-counters    Ingress counters group configuration
  interface           Interface infomation
  ip                  IP information
  ip-sla              Internet Protocol Service Level Agreement
OS900(config)# i
```

Notice that the four commands **`igmp`**, **`ingress-counters`**, **`interface`**, and **`ip`** are displayed because all four of these commands begin with '`i`'. To select the command **`interface`** type the letters '**`nt`**',so as to have '**`int`**' which distinguishes it from the other commands, and press Tab. The CLI response is shown below.

```
OS900(config)# interface
```

Press Shift ? to display the selectable arguments. The CLI response is shown below.

```
OS900(config)# interface ?
  IFNAME       Existing interface device-name (i.e vif3,...)
  out-of-band  New or existing out-of-band interface configuration
  vlan         New or existing vlan interface configuration
OS900(config)# interface
```

Select '`vlan`' by typing **`v`** and pressing Tab. The CLI response is shown below.

```
OS900(config)# interface vlan
```

Press Shift ? to display the selectable arguments. The CLI response is shown below.

```
OS900(config)# interface vlan ?
  IFNAME  Interface device-name as vif# (i.e vif3 )
OS900(config)# interface vlan
```

Type an interface ID, e.g., **`vif7`**, and press Shift ? to display the selectable arguments. The CLI response is shown below.

```
OS900(config)# interface vlan vif7 ?
  <cr>
  |     Output modifiers
OS900(config)# interface vlan vif7
```

Notice that only the symbols '`<cr>`' and '`|`' appear. This indicates that there are no more arguments to enter.

To invoke the command, press the Enter. The CLI response is shown below.

```
OS900(config)# interface vlan vif7
OS900(config-vif7)#
```

Notice that the system prompt has changed from '`OS900(config)#`' to '`OS900(config-vif7)#`', indicating that the command was successfully executed and that the system has entered '`interface`' mode.

# Quick Entry of a CLI Command

For convenience, to invoke a command it is sufficient to type only the first few letters of the command that are different from the other commands (and to press Enter).

<u>Example</u>
For e.g., if the only commands in a mode that begin with the letter 'e' are **enable** and **exit**, to invoke enable it is enough to type **en**; to invoke exit it is enough to type **ex**.

# Negation of CLI Command

Many commands may be prefixed with **no** in order to disable the feature or function enabled by the command. By invoking the command *without* the prefix **no**, the function (not data) that you disabled (or that was disabled) is re-enabled.

<u>Example</u>
The command **lt aging** *enables* aging out of entries in the Learn Table.
The command **no lt aging** *disables* aging out of entries about stations in the Learn Table.

# Viewing Modes

Viewing of system information on the screen can be set to either of the following formats:

– Paging (display one full screen of information at a time)
– No paging (display all information without interruption until its end)

## Paging

This is the default method.

1. Enter **enable** mode.
2. Invoke the command **cli-paging**.

## No Paging

1. Enter **enable** mode.
2. Invoke the command **no cli-paging**.

# Pipelining a CLI Command

The pipe **|** is used to process the output of a CLI command (e.g., **show lt**) by a Linux command (e.g., **wc**, **grep**, **tail**, etc.).

<u>Example</u>

```
OS900(config)# show lt | ?

  ..       Shell command to process the output
  begin    Begin with the line that matches
  end      End with the line that matches
  exclude  Exclude line that match
  include  Include line that match
  write    Write output to file
OS900(config)# show lt | begin B8 2
3       00:0F:BD:00:05:B8  1    Intern STATIC
7       FF:FF:FF:09:BD:5C  1    Intern STATIC
OS900(config)#
```

where,

**B8** is the pattern that a line must contain in order to be displayed. **2** is the number of lines to be displayed. 3 and 7 are the entry numbers in the Learn Table.

<u>Example</u>

```
OS900# show lt | wc
     18      78     933
OS900#
```

where,

`lt` is Learn Table, `wc` is word count, `18` is the number of lines, `78` is the number of words, `933` is the number of characters.

Example

This example shows how to display the lines containing the string **`7C:22:8A:B5:16:CE`** in the output of the command **`show lt`**, and the word count of these lines.

```
OS900# show lt | grep 7C:22:8A:B5:16:CE
2       7C:22:8A:B5:16:CE  1    Intern STATIC
4       7C:22:8A:B5:16:CE  100  Intern STATIC
42      7C:22:8A:B5:16:CE  4095 Intern STATIC
OS900# show lt | grep 7C:22:8A:B5:16:CE | wc
      3      15     150
OS900#
```

where,

`lt` is Learn Table, `wc` is word count. `2`, `4`, and `42` are the entry numbers in the Learn Table. `3` is the number of lines, `15` is the number of words, `150` is the number of characters.

Example

To display the first 10 entries of the MAC table containing the string `00:60`, do:

```
OS900# show lt | include 00:60 | head -n 10
OS900#
```

No entry is displayed because no entry containing the string `00:60` exists.

# Accessing an *enable* Mode Command from any Mode

From any mode, any command in **`enable`** mode can be accessed by prefixing the command with **`do`**.

Example

To invoke the command **`show time`** (which is in **`enable`** mode) from the mode **`interface`**, invoke **`do show time`** as shown below:

```
OS900> enable
OS900# configure terminal
OS900(config)# interface vlan vif7
OS900(config-vif7)# do show time
Tue Aug 19 21:17:15 GMT 2008
OS900(config-vif7)#
```

# Alias

An alias is a user-assigned alternate name for an existing CLI command.

Any CLI command (including *Scripts*, page *118*), in any mode can be assigned an alias.

An alias serves two purposes:

- As a mnemonic (for conveniently identifying the command)
- Quickly invoking the command by entering only its name

## Viewing

To view an alias of a command, invoke the command:

**`show alias [all|this|NODENAME [NAME]]`**

where,

**`all`**: In all modes

**`this`**: In current mode

**`NODENAME`**: Name of a mode in which the alias is to apply

**`NAME`**: Alias (alternate name for the command)

## Assigning

To *assign* an alias to a command, invoke the following command:

**alias all|this|NODENAME NAME Command text**

where,

**all**: In all modes

**this**: In current mode

**NODENAME**: Name of a mode in which the alias is to apply

**NAME**: Alias (alternate name for the command)

**Command text**: CLI command with argument values, if any

In the example below, although the alias is assigned in **configure terminal** mode it can be used to invoke the CLI command in any mode.

Example

```
OS900(config)# alias
  all       In all nodes
  this      In current node
  NODENAME  Node name
OS900(config)# alias all
  NAME  Name of alias
OS900(config)# alias all INF
  ..  Command text
OS900(config)# alias all INF show interface vif29
OS900(config)#
```

## Invoking

To *invoke* a command simply use its alias as the command.
In the example below, the alias is invoked in **enable** mode although it was assigned in **configure terminal** mode.

Example

```
OS900# INF
alias(INF) => show interface vif29

Name    M Device       IP               State MAC              Tag  Ports
-------------------------------------------------------------------------------
vif29     vif29        -                 DO   00:0F:BD:00:5E:A1 0347 5-8

OS900#
```

## Deleting

To delete an alias, invoke the command:

**no alias all|this|NODENAME NAME [Command text]**

where,

**all**: In all modes

**this**: In current mode

**NODENAME**: Name of a mode in which the alias is to apply

**NAME**: Alias (alternate name for the command)

**[Command text]**: CLI command with argument values, if any

# Copy-Paste Mode

## General

In Copy-Paste mode a set of CLI commands are automatically executed simply by pasting them onto a CLI window in the *appropriate* commands mode (possibly **`configure terminal`** mode).

## Usage

The procedure for using the **`copy-paste`** feature is as follows:

1. Enter the mode in which the CLI commands are to be pasted and automatically executed.
2. Paste the CLI commands onto the CLI window.

## Example

The example below demonstrates how the command **`copy-paste`** can be used to configure VLAN interfaces.

```
-------------------------------------------------------Viewing configured interfaces -------------------------------------------------------

OS900# show interface

INTERFACES TABLE
================
Name     M Device       IP                 State MAC               Tag  Ports
-------------------------------------------------------------------------------
vif0       vif0         -                   DO    00:0F:BD:00:05:B8 0001 1-10

- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

------------------------Entering the mode in which the commands are to be pasted and executed------------------------

OS900# configure terminal
OS900(config)#

--------------------------------------------------Pasted commands to be executed--------------------------------------------------

interface vlan vif1
 tag 10
 ip 193.218.67.55/24
 ports 1-2
interface vlan vif2
 tag 20
 ip 193.88.67.55/24
 ports 3-4

----------------------------------------------------------------Executed  commands----------------------------------------------------------------

OS900(config)# interface vlan vif1
OS900(config-vif1)#  tag 10
OS900(config-vif1)#  ip 193.218.67.55/24
 OS900(config-vif1)#  ports 1-2
Interface is activated.
OS900(config-vif1)# interface vlan vif2
OS900(config-vif2)#  tag 20
OS900(config-vif2)#  ip 193.88.67.55/24
OS900(config-vif2)#  ports 3-4
Interface is activated.
OS900(config-vif2)#
```

```
----------------------------------Viewing the results of the execution of the pasted commands----------------------------------

OS900(config-vif2)# exit
OS900(config)# show interface

INTERFACES TABLE
================
Name     M Device        IP                 State MAC               Tag  Ports
-------------------------------------------------------------------------------
vif1       vif1          193.218.67.55/24    DO   00:0F:BD:00:36:67 0010 1-2
vif2       vif2          193.88.67.55/24     DO   00:0F:BD:00:36:67 0020 3-4
vif0       vif0          -                   DO   00:0F:BD:00:36:67 0001 5-10

- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

OS900(config)#
```

# Linux Mode

## General

The OS900 Master-OS™ software runs over the Linux operating system. The user can access the Linux operating system shell in order to perform advanced functions and to monitor internal Master-OS™ operations and parameter values.

| | |
|---|---|
| ⚠ | **CAUTION!**<br>Before accessing the Linux operating system shell, it is advisable to consult Customer Support at MRV.<br>Improper use of the shell/Linux commands at the SuperUser level may cause damage to the OS900 Master-OS™ software and OS900 File System! |

## Entry

The procedure for accessing the Linux operating system shell is as follows:

1. Enter **enable** mode.
2. To enter Linux mode, type **linux**.
3. When the prompt **$** appears, invoke the command **su** for superuser privileges.
4. When the prompt `Password:` appears, type the *root* password. If no *root* password was configured, the default is no password. In such case, simply press Enter.

Example

```
OS900> enable
OS900# linux
$ su
Password:
#
```

## Exit

To exit the Linux operating system shell, type **exit** twice.

Example

```
# exit
exit
$ exit
exit
OS900#
```

# Passwords

Four passwords can be configured for the OS900, each corresponding to a different access level. The access levels are described in the section *Access Levels*, page *87*. The passwords are:

- **Admin Password**
  Enables access to general display and external connectivity CLI commands of the OS900
- **Enable Password**
  Enables access to Admin Level and general system CLI commands of the OS900
- **Configure Password**
  Enables access to system operation configuration CLI commands of the OS900
- **Root Password**
  Enables access to the (Linux) operating system of the OS900

Root and Admin passwords, by default, are encrypted. Encryption of an Enable or Configure password is optional.

## Changing the Root Password (and Admin Password)

The root and admin passwords are configured at first time login as described in the section *First Time Access – Root and Admin Passwords Configuration*, page *88*. To change the root and admin passwords:

1. Boot or reboot the OS900.
2. Enter **enable** mode.
3. Type **linux**[12].
4. When the prompt `$` appears, type **su** (SuperUser).
5. When the prompt `password:` appears, type the *root* password. If no root password was configured, the default is no password. In such case, simply press Enter.
6. When the prompt `#` appears, type **set_fb**.
7. Reboot the OS900 by typing reboot.

The OS900 starts rebooting. At the end of the reboot process, the following prompt is displayed:

```
MRV OptiSwitch 910 version 1-0-0
OS900 login:
```

8. Configure new *root* and *admin* passwords as described in the section *First Time Access – Root and Admin Passwords Configuration*, page *88*.

Below is an example showing the user inputs (in **bold**) for changing the *root* and *admin* passwords and OS900 outputs on the CLI screen. The string of asterisks shown as user password is only a representation of the password; the password is actually hidden from view during entry.

```
OS900> enable
OS900# linux
$ su
Password: ******
# set_fb
# reboot
........................
........................
....................
MRV OptiSwitch 910 version 1_0_10
OS900 login:
```

[12] Entry to the linux mode is indicated by the prompt `$`. To exit linux mode, invoke the command **exit**.

## Changing only the Admin Password

The Admin password is configured the first time the OS900 is accessed, as described in the section *First Time Access – Root and Admin Passwords Configuration*, page *88*. To change the password:

1. Enter **enable** mode as follows:

```
OS900> enable
OS900#
```

2. Enter **configure terminal** mode as follows:

```
OS900# configure terminal
OS900(config)#
```

3. Type **password** and press Enter. The following prompt appears:

```
OS900(config)# password
Changing password for admin
(current) UNIX password:
```

4. Enter the old (current) password and press Enter. If no admin password was configured, the default is no password. In such case, simply press Enter. The following prompt appears:

```
Enter new UNIX password:
```

5. Enter your new password. The following prompt appears:

```
Retype new UNIX password:
```

6. Re-enter the new password. The password is authenticated and, if accepted by the system, the following prompt appears:

```
OS900(config)#
```

7. In order to store the password in permanent memory, invoke the command **write file** or **write memory**.

## Configuring/Changing the Enable Password

1. Enter **enable** mode.

```
OS900> enable
OS900#
```

2. Enter **configure terminal** mode.

```
OS900# configure terminal
OS900(config)#
```

3. Invoke the command:

   **enable password PASSWORD**

   where,

   **PASSWORD**: Password.

```
OS900(config)# enable password myEnablePass
```

4. In order to save the password to the configuration files, invoke the command:

   **write file**

   or

   **write memory**

The command **write terminal** shows the password.

Example

```
MRV OptiSwitch 910 version 1-0-10
OS900 login: admin
Password:
Last login: Thu Sep 1 06:58:43 2006 on ttyS0

OS900> enable
OS900# configure terminal
OS900(config)# enable password myEnablePass
OS900(config)# service password-encryption
OS900(config)#
OS900(config)# write terminal
Building configuration...

Current configuration:
! version 1_0_10
enable password 8 iBZPg9fiHT9RQ
service advanced-vty
service password-encryption
OS900(config)#
```

The example above shows the password **myEnablePass** encrypted as `iBZPg9fiHT9RQ`.

## Configuring/Changing the Configure Password

1. Enter **enable** mode.

```
OS900> enable
OS900#
```

2. Enter **configure terminal** mode.

```
OS900# configure terminal
OS900(config)#
```

3. Invoke the command:

    **configure password WORD**

    where,

    **WORD**: Password.

```
OS900(config)# enable password myConfigurePass
```

4. In order to save the password to the configuration files, invoke the command:

    **write file**

    or

    **write memory**

The command **write terminal** shows the password.

Example

```
MRV OptiSwitch 910 version 1-0-0
OS900 login: admin
Password:
Last login: Thu Sep 1 06:58:43 2006 on ttyS0

OS900> enable
OS900# configure terminal
OS900(config)# configure password myConfigurePass
OS900(config)# service password-encryption
OS900(config)#
OS900(config)# write terminal
Building configuration...

Current configuration:
! version 1_0_10
configure password 8 t0RcxPg9fiNT9bd
service advanced-vty
service password-encryption
OS900(config)#
```

The example above shows the password **myConfigurePass** encrypted as `t0RcxPg9fiNT9bd`.

## Deleting the Enable Password

To delete the enable password, enter mode **configure terminal** and invoke the command:

**no enable password**

To implement deletion of enable password in permanent memory invoke the command:

**write file**

or

**write memory**.

## Deleting the Configure Password

To delete the enable password, enter mode **configure terminal** and invoke the command:

**no configure password**

To implement deletion of enable password in permanent memory invoke the command:

**write file**

or

**write memory**.

## Encrypting Passwords

### Enabling

To *enable* encryption of the **enable** mode password and **configure terminal** mode password, and passwords associated with ISIS, BGP, and MPLS-implemented LDP:

1. Enter **configure terminal** mode
2. Invoke the command:

   **service password-encryption**

Example

```
OS912C(config)# service password-encryption
OS912C(config)#
```

### Disabling

To *disable* encryption of the **enable** mode password and **configure terminal** mode password, and passwords associated with ISIS, BGP, and MPLS-implemented LDP – *as well as to also delete the* **enable** *mode password*:

1. Enter **configure terminal** mode
2. Invoke the command:

   **no service password-encryption**

Example

```
OS912C(config)# no service password-encryption
OS912C(config)#
```

# Viewing Installed Components

## Hardware and Software

To view *what* hardware and software components are installed in the OS900 and what features are supported, from any mode invoke the command:

**show version**

Example

```
OS910> enable
OS910# show version

MRV OptiSwitch 910
=========================
Hardware
--------
Board serial number: 0647002339
CPU serial number  : 0647002676

CPU: MPC8245, 266MHz with 64MB flash and 256MB Dram memory
CPU Hardware: id 3, version 1
Device Hardware version: 5
Device temperature: 40C / 104F (normal)

Power Supplies:
unit 1 AC: INSTALLED & ACTIVE  (hw-type 1)

Fans:
Fan 1: NOT ACTIVE

Valid ports: 1-10

Software
--------
MasterOS version: 2_1_1
Build time: Sun Jul  6 15:36:59 IDT 2008
Based on:
Linux OS910 2.6.15 #413 Thu Jun 26 15:18:10 IDT 2008 ppc
ZebOS 5.2 (powerpc-603-linux-gnu).
Driver v1.4 mvPp s6352  PLD 4  sHwVer 1

Base MAC address: 00:0F:BD:01:36:67

Supported features:
-------------------
MSTP -     Yes
ROUTING -  Yes
RIP -      Yes
```

```
OSPF -      Yes
ISIS -      Yes
BGP -       Yes
MPLS -      No
LDP -       No
RSVP -      No
WEB -       No
IPv6 -      No

up   0:10, 1 user
OS910#
```

### Backup Image

To view the version of the backup image of the OS900:

1. Enter **enable** mode
2. Invoke the command:
   **show version backup**

Example

```
OS900# show version backup
Wait please, while retrieving backup version...
MasterOS version: 2_1_1
OS900#
```

The procedure for loading the backup image is given in section *Running the Backup Image*, page *516*.

### CPU

To view information about the OS900 CPU:

1. Enter **enable** mode.
2. Invoke the command **show cpu**.

Example

```
OS900# show cpu
processor       : 0
cpu             : 82xx
revision        : 16.20 (pvr 8081 1014)
bogomips        : 175.71
vendor          : Motorola SPS
machine         : MRV SBC
```

## Remote Management Access

Management access to the OS900 can be gained via one or more interfaces, e.g., Serial/RS-232 interface **CONSOLE EIA-232**, out-of-band IP interface **MGT ETH**, or an inband IP interface.

Remote management access to the OS900 via its IP interfaces (using an SNMP, TELNET, or SSH connection) is, by default, disabled. Access may be enabled out-of-band and/or inband and selectively for SNMP, TELNET, and/or SSH.

To enable out-of-band or inband remote management, refer to the section *Remote Management*, page *191*.

## Hostname

The hostname of an OS900 is its network name.

### New

To change the hostname of an OS900:

1. Enter **configure terminal** mode

2. Invoke the command:
   **hostname WORD**
   where,
   **WORD**: Hostname. Only a string without any blanks in it is allowed. The string can be built with words interconnected with underscores and/or hyphens in order to make it more intelligible. The words may include uppercase and lowercase letters.

Example

```
OS900(config)#hostname Zeus_2
zeus_2(config)
```

## Default

The default hostname is the factory-set name. The name is usually the model of the OS900. To change the hostname to the default:

1. Enter **configure terminal** mode
2. Invoke the command:
   **default hostname**
   or
   **no hostname**

Example

```
Zeus_2(config)# default hostname
OS910(config)#
```

# Banner

## Definition

A banner is text indicating the OS900's association. The banner can consist of one or more text lines and appears on the console at login.

## Default

The default banner is the factory-set banner that usually identifies the vendor name, product, and operative software version.

Example

```
MRV OptiSwitch 910 version os900-2-1-0-d30-07-08-0800
```

## Viewing

To view the current banner, from **enable** mode invoke the command **show banner**.

## Configuring

### Method 1

To configure the *first* line of the banner:

1. Enter **configure terminal** mode.
2. Invoke the command **banner TEXT**
   where,
   **TEXT**: Text to be entered in the banner line.

To configure *additional* lines in the banner:

1. Invoke the command **banner-line NUMBER TEXT**
   where,
   **NUMBER**: Number of banner line.

**TEXT**: Text to be entered in the banner line.

2. Repeat the above command for each banner line you want.

Example

```
OS900(config)# banner MRV OptiSwitch 910 version 1-0-0
OS900(config)# banner-line 2 Hamelyn Town
OS900(config)# banner-line 3 Building Complex 25G
OS900(config)# show banner
Line  1 : MRV OptiSwitch 910 version d1734-22-09-05
Line  2 : Hamelyn Town
Line  3 : Building Complex 25G
OS900(config)#
```

**Method 2**

To configure a banner consisting of multiple lines:

1. Enter **configure terminal** mode.
2. Enter **banner** mode.
3. Type text to be entered in the first, second, etc. banner line making sure to press Enter at the end of each line.

Example

```
OS900# show banner
banner is default
OS900# configure terminal
OS900(config)# banner
OS900(config-banner)# MRV OptiSwitch 910 version 1-0-0
OS900(config-banner)# Hamelyn Town
OS900(config-banner)# Building Complex 25G
OS900(config-banner)# exit
OS900(config)# exit
OS900# show banner
Line  1 : MRV OptiSwitch 910 version d1734-22-09-05
Line  2 : Hamelyn Town
Line  3 : Building Complex 25G
OS900(config)#
```

# Date

To configure/change the date, from **enable** mode type **date** and enter the month, day, and year.

Example

```
OS910# date sep 01 2008
OS910#
```

# Time

To configure/change the local time, from **enable** mode type **time TIME** and enter the time in hours, minutes, and, optionally, in seconds in the format **hh:mm[:ss]**.

Example

```
OS910# time 14:28:35
OS910#
```

# Location

To configure/change the location/site record of the OS900:

1. Enter the following modes in succession:

   **enable → configure terminal → snmp**

   Example

```
OS900(config)#snmp
```

```
OS900(config-snmp)
```

2. Type **`location`** and the location description. The description can be any alphanumeric string. The string can be a single word or several words separated by blank spaces or interconnected with hyphens and/or underscores.

Example

```
OS900(config-snmp)location main_building_second_floor
OS900(config-snmp)
```

# Rebooting

Rebooting restarts the OS900 with the new image (operative firmware) if one was downloaded or with the existing image.

## Modes

The OS900 can be set so that at reboot it is either configured or not configured according to its configuration file **`system.conf`**.

By default, the OS900 is configured according to its configuration file at reboot.

### Without Configuration File

To set the OS900 so that it is *not* configured according to its configuration file at reboot:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`boot-config-file empty-configuration`**

### With Configuration File

To set the OS900 so that it is configured according to its configuration file at reboot:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`default boot-config-file`**

## Methods

The OS900 can be rebooted at any time using any of the following methods:

### Normal

1. Enter **`enable`** mode.
2. Invoke the command:
   **`reboot`** if you want to reconsider whether to reboot.
   In response to the prompt:
   `Would you like to reboot the system now ? (y|n)`
   Type **`y`** if you want to reboot now.
   Type **`n`** if you do *not* want to reboot.
   Or
   **`reboot-force`** if you want rebooting to be done straightaway, i.e., without prompts.

### Warm

To restart the OS900 system *without* powering it OFF and ON, press pushbutton ***PWR***.

### Cold

To restart the OS900 system *with* powering it OFF, press pin pushbutton ***RST***.

### Scheduler

Use the Scheduler utility *Scheduler*, page *499*. This utility can be used to automatically trigger rebooting at a *preset* date and time.

# Learn Table

## Definition

The Learn Table is a map of currently connected stations[13] to ports. The Learn Table is dynamically updated and can maintain as many as 16K unicast entries (MAC addresses) for an OS900.

## Viewing

All or selective entries of the Learn Table can be displayed according to one or more of the following attributes: port number, tag number, interface ID.

To view Learn Table entries:

1. Enter **enable** mode.
2. To view entries using interface ID:
   Invoke the command:
   **show lt port PORT|all interface IFNAME|all**
   where,
   **PORT**: Port number.
   **all**: (first) All ports.
   **IFNAME**: ID of an existing interface (e.g., **vif3**)
   **all**: (second) All interfaces.

   To view entries using interface Tag:
   Invoke the command:
   **show lt port PORT|all tag TAG|all**
   where,
   **PORT**: Port number.
   **all**: (first appearance) All ports.
   **TAG**: Tag of existing interface (e.g., **vif3**)
   **all**: (second appearance) All tags.

   To view *all* entries:
   Invoke the command:
   **show lt**

## Learning

To enable learning of MAC addresses of stations whose traffic is received by the OS900:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **lt learning**

Example

```
OS906C(config)# lt learning
OS906C(config)#
```

To disable learning:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no lt learning**

Example

```
OS906C(config)# no lt learning
OS906C(config)#
```

[13] The stations are identified by their MAC address.

## Aging

### General

Aging is a mechanism that clears entries of stations that are not active, shutdown, or moved to another location. The default aging time is 300 seconds.

### Custom

To change the aging time:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`lt aging <10-630>`**
   where,
   **`<10-630>:`** Aging time in seconds. The aging time must be a number that is a multiple of 10 and in the range **`10-630`**.
   **`default:`** Default aging time (300 seconds).

Example

```
OS900(config)# lt aging 370
OS900(config)#
```

### Default

To set the aging time to the default value:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`lt aging default`**
   where,
   **`default:`** Default aging time (300 seconds).

### Disabling

To disable aging:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`no lt aging`**

Example

```
OS900(config)# no lt aging
OS900(config)#
```

## Limiting

Logging of entries in the Learn Table can be limited in number with respect to pre-specified ports of entry and VLAN tags. If the limit is reached, new MAC address will not be learned. However, frames with new MAC addresses (i.e., MAC addresses that do not exist in the Learn Table when it has become full) will, *by default*, flood. To cause frames with new MAC addresses to be dropped invoke the command described in the section *Dropping*, page *113*.

To limit entries *with respect to* ports:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`lt limit port PORTS-GROUP entries ENTRIES-LIMIT`**
   where,
   **`PORTS-GROUP:`** Group of ports.
   **`ENTRIES-LIMIT:`** Maximum number of entries in the range **`0-16k`** that may be logged in the Learn Table. (**`16k`** is decimal 16000). This number applies for each individual port in the group.

   To revoke limiting with respect to ports, invoke the command:
   **`no lt limit port PORTS-GROUP`**

Example

```
OS900(config)# lt limit port 4-7 entries 6k
OS900(config)#
```

To limit entries *with respect to* VLAN tags:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **lt limit tag TAGS-GROUP entries ENTRIES-LIMIT**

   where,

   **TAGS-GROUP:** VLAN tags in the range **0-4095**.

   **ENTRIES-LIMIT:** Maximum number of entries in the range **0-16k** that can be logged in the Learn Table.

   To revoke limiting with respect to tags, invoke the command:

   **no lt limit tag TAGS-GROUP**

Example

```
OS900(config)# lt limit tag 2-10 entries 5k
OS900(config)#
```

To view the limits on entries (*with respect to* ports and VLAN tags):

1. Enter **enable** mode.
2. Invoke the command:

   **show lt limit**

Example

```
OS900# show lt limit
NO PORTS      TAGS       LIMIT
1  -          2-10       5120
2  4-7                   6144
OS900#
```

## Dropping

To cause frames whose MAC addresses do not exist in the Learn Table when it has become full to be dropped, invoke the command:

**lt limit action drop PORTS-GROUP|all**

where,

**PORTS-GROUP**: Group of ports.

**all**: All ports.

Example

```
OS900(config)# lt limit action drop 3-7,9
OS900(config)#
```

## Adding Entries Manually

Entries may be added manually in the Learn Table as follows:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **lt entry MAC_ADDRESS PORT TAG dynamic|static [<0-7>]**

   where,

   **MAC_ADDRESS:** Learned MAC address in the format **xx:xx:xx:xx:xx:xx**, where **xx** is a double-digit hexadecimal number.

   **PORT:** Physical port number.

   **TAG:** Interface VLAN tag in the range **1-4095**.

   **dynamic:** Dynamic entry, i.e., the entry *can* be aged out.

   **static:** Static entry, i.e., the entry *cannot* be aged out. Static entries are not stored in the configuration file, **system.conf**, so that they are lost on reboot.

**[<0-7>]**: Traffic-class priority for a packet with this destination MAC address. Default: **0**, i.e., lowest priority

To remove a logged entry, invoke the command:

**no lt entry MAC_ADDRESS TAG**

Example

```
OS900(config)# lt entry 7b:22:c9:3d:5e:ab 6 30 dynamic 4
OS900(config)#
```

## Policing

The policing action (forward or drop) can be performed on ingress packets based on the Source or Destination MAC address and on whether the Learn Table entry is static or dynamic.

To apply the policing policy:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **lt entry MAC_ADDRESS PORT TAG dynamic|static sa-action fwd|drop [da-action fwd|drop]**

   where,

   **MAC_ADDRESS**: Learned MAC address in hex format, e.g., aa:bb:cc:dd:ee:ff
   **PORT**: Egress physical port for the packet
   **TAG**: VLAN ID of the ingress packet
   **dynamic**: Dynamic entry, i.e., the entry *can* be aged out.
   **static**: Static entry, i.e., the entry *cannot* be aged out.
   **sa-action**: For Source MAC address
   **da-action**: For Destination MAC address
   **fwd**: Forward packets with this source MAC
   **drop**: Drop packets with this source MAC

## Flushing

### Port Entries

To cause existing entries for a port in the Learn Table to be flushed when the port link goes down:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **lt clear-port-link-down**

Example

```
OS900(config)# lt clear-port-link-down
Tag limit cannot be set with clear port.
OS900(config)#
```

### All Entries

To delete all existing entries in the Learn Table:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **clear lt**

Example

```
OS900(config)# clear lt
OS900(config)#
```

# Maximum Transmission Unit (MTU)

## General

This section defines and shows how to set the Maximum Transmission Unit (MTU) for ports and VLAN interfaces of the OS900. MTUs can also be set for traffic shaping (as described in the section*Maximum Transmission Unit (MTU) for Port Shaper* , page *376*) and for Traffic Conditioners (as described in the section *Maximum Transmission Unit (MTU) for Policing*, page *360*.)

## Definition

MTU is the largest physical packet size (possibly jumbo packet size) that specific ports or VLAN interfaces of the OS900 will forward.

## Applicability

An MTU size can be set for each port (trunk port as well) independently. An MTU is set for a VLAN interface by assigning an MTU profile to the VLAN interface. Up to eight MTU profiles (MTU sizes) can be defined for assignment to VLAN interfaces. An MTU profile can be assigned to several VLAN interfaces. Only one MTU profile can be assigned to a VLAN interface. The MTU set for a VLAN interface will apply for all ports that are members of the VLAN interface.

> **Note**
>
> If different MTUs are defined for a VLAN interface (as described in the section *Setting for Ports*, page *115*), member ports (as described in the section *Setting for VLAN Interfaces*, page *115*), and CPU (as described in the section *Configuring*, page *181*, Step *8*) the smallest of the MTUs will be selected by the OS900.

## Setting for Ports

To set an MTU to a *group of ports*:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port mtu-size PORTS-GROUP|all <64-16000>`**

   where,

   **`PORTS-GROUP:`** Group of ports.

   **`all:`** All ports.

   **`<64-16000>:`** Range of MTUs in bytes.

Example

```
OS900(config)# port mtu-size 1-3 3019
OS900(config)#
```

## Setting for VLAN Interfaces

Before setting an MTU for a VLAN interface, a profile (number) must be defined for the MTU.

To *define* a profile for a VLAN interface:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`vlan-mtu-profile profile <1-8> <64-16000>`**

   where,

   **`<1-8>:`** Range of MTU profiles.

   **`<64-16000>:`** Range of MTUs in bytes.

Example

```
OS900(config)# vlan-mtu-profile profile 3 8157
OS900(config)#
```

To set an MTU for a VLAN interface *assign* an MTU profile to the VLAN interface as follows:

1. Enter the mode of the VLAN interface.
2. Invoke the command:

   **`mtu-profile <1-8>`**

   where,

   **`<1-8>:`** Range of MTU profiles.

# Syslog

## Definition

Syslog is a standard logging mechanism that stores system messages and events.

Events for all processes except for the Operative Software are, by default, logged in Syslog. The procedure for enabling the OS900 to log Operative Software events as well in the Syslog is given in the section *Logging of Events*, page *116*.

## File Location

The *internal* Syslog file is stored at: **/var/log/messages**.

The *remote* Syslog file is stored on the Remote Syslog server.

## Logging of Events

By default, events are logged in Syslog for all processes except for the Operative Software. To enable logging of Operative Software events as well:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`log syslog [trap alerts|critical|debugging|disable|emergencies|errors| informational|notifications|warnings]`**

   where,

   **`alerts:`** Log alerts, emergencies

   **`critical:`** Log critical errors, alerts, emergencies

   **`debugging:`** Log debugging messages, informational messages, notifications, warnings, errors, critical errors, alerts, emergencies

   **`disable:`** Do not log *any* event

   **`emergencies:`** Log emergencies

   **`errors:`** Log errors, critical errors, alerts, emergencies

   **`informational:`** Log informational messages, notifications, warnings, errors, critical errors, alerts, emergencies

   **`notifications:`** Log notifications, warnings, errors, critical errors, alerts, emergencies

   **`warnings:`** Log warnings, errors, critical errors, alerts, emergencies

## Default Mode

To set Syslog to the default mode:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`no log syslog`**

## Logging of CLI Commands

### Enabling

To enable logging of executed CLI commands in Syslog:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`log commands`**

### Disabling

By default, logging of executed CLI commands in Syslog is disabled.
To disable logging of executed CLI commands in Syslog:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`no log commands`**

## Viewing

To view Syslog messages:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show syslog [all|debug|info|warning|error|fatal] [START_DATE] [END_DATE]`**
   where,
   **`all:`** Show all messages
   **`debug:`** Show messages in the range debug level to fatal level
   **`info:`** Show messages in the range info level to fatal level
   **`warning:`** Show messages on the levels warning, error, and fatal
   **`error:`** Show messages on the levels error and fatal
   **`fatal:`** Show only messages with level fatal
   **`START_DATE:`** The start date. Format: `mm-dd-hh:mm:ss`, e.g., **`04-01-09:00:00`** or **`start`** for messages from the beginning.
   **`END_DATE:`** The end date. Format: `mm-dd-hh:mm:ss`, e.g., **`04-01-09:00:00`** or **`exclude`** for messages ending at current time.

## Clearing

To clear the internal Syslog file:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`clear syslog`**

## Remote Syslog

### General

Syslog is maintained in the OS900 RAM and is erased on power off or reboot. To keep a permanent record of the Syslog, a Remote Syslog server can be used, such as, a PC running a Syslog application program.

### Requirements

The following are required for Remote Syslog:

- Syslog Server
  (For e.g., PC with the following:
  – Operating System: For e.g., Microsoft Windows 95/98/2000/NT/XP
  – Syslog application program: For e.g., 3Com 3CSyslog
- Connectivity of the OS900 to the Syslog server.

**Setup**

***Enabling***

To enable *Remote* Syslog:

1. Verify connectivity to the Syslog server, for e.g., by invoking the command **`ping`** in **`enable`** mode
2. Enter **`configure terminal`** mode.
3. Invoke the command:

   **`rsyslog IPV4_ADDRESS [IPV4_ADDRESS]`**

   where,

   **`IPV4_ADDRESS:`** IP address of first Syslog server

   **`[IPV4_ADDRESS]:`** IP address of second Syslog server

***Disabling***

To disable *Remote* Syslog:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`no rsyslog`**

# Scripts

## Definition

A Script is a set of factory CLI commands that the OS900 can execute in succession without user intervention. Once a script is defined, it can be used just like any other CLI command.

## Purpose

The Script utility is used to make the configuration procedure for the OS900 simpler and quicker for technicians in the field.

## Structure

A script consists of the following:

- Parameters (script arguments)
- Lines (a sequence of CLI commands that may include script Parameters as arguments)

## Creating

To create a script, you basically need to do the following:

- Create Parameters
- Create Lines (that contain factory CLI commands) with the appropriate Parameters

A Script is created as follows:

1. Enter **`configure terminal`** mode.
2. Assign a name to the script by invoking the command:

   **`script NAME`**

   where,

   **`NAME`**: Name of script.
   String of up to *thirteen* alphanumeric characters.
   Letter characters must be lowercase only and must not be blanks, e.g., **`ipiface01`**.
3. Optionally, enter a textual description of the script by invoking the command:

   **`description TEXT`**

   where,

**TEXT**: Description of script. Text that can include blanks.

4. Create the parameters as described in the section *Create Parameter*, page *119*.
5. Create the lines with CLI commands as described in the section *Create Line*, page *121*.

## Parameters

Parameters are script arguments. The user can define a list of Parameters that can be later used in Lines of a script.

The actions that can be performed on a *parameter* are as follows:

- Create Parameter
- View Parameter
- Modify Parameter
- Delete Parameter

### Create Parameter

To create a parameter:

1. Enter **configure terminal** mode.
2. Enter the mode of a script (existing or new) by invoking the command:

   **script NAME**

   where,

   **NAME**: Name of script. String of up to thirteen alphanumeric characters. Letter characters must be lowercase only and must not be blanks, e.g., **ipiface01**.
3. Invoke the command:

   **parameter [NUMBER] NAME type TYPE description TEXT**

   where,

   **NUMBER**: (optional) Index of parameter. Set the order of the parameter. If not specified, a number that is a multiple of 10 (e.g., 10, 20, 30, etc.) is assigned.

   **NAME**: Name for the parameter.

   **TYPE**: Type for parameter.

   **TEXT**: Description for parameter.

Example

```
OS900# configure terminal
OS900(config)# script ipiface01
OS900(script-ipiface01)# parameter 10   IFID type vifN description Vlan Interface ID
OS900(script-ipiface01)#
```

### View Parameter

The procedures for viewing a Parameter are the same as those given for viewing a Script – see section *Viewing*, page *122*.

### Modify Parameter

To modify the name, type, or description of a parameter:

1. Enter the mode of the script containing the parameter to be modified by invoking the command:

   **script NAME**

   where,

   **NAME**: Name of script.
2. Invoke the command:

   **parameter NUMBER NAME type TYPE description TEXT**

   where,

   **NUMBER**: Number of the parameter whose name, type, or description is to be changed.

   **NAME**: New name for the parameter.

**TYPE**: New Type for parameter.

**TEXT**: New description for script.

### Delete Parameter

To delete a parameter from an existing script:

1. Enter **configure terminal** mode.
2. Enter the mode of the script containing the parameter to be deleted by invoking the command:

   **script NAME**

   where,

   **NAME**: Name of script.
3. Invoke the command:

   **no parameter NUMBER**

   where,

   **NUMBER**: Number of the parameter to be deleted.

Example

```
OS900(script-IpInterface01)# no parameter 30
OS900(script-IpInterface01)#
```

### Renumber Parameters

To renumber all Parameters (and Lines) of a script with the sequence 10, 20, 30, etc.:

1. Enter the mode of the script by invoking the command:

   **script NAME**

   where,

   **NAME**: Name of script.
2. Renumber the Parameters (and Lines) by invoking the command:

   **renumerate**

Example

The example below shows that the numbers of the Parameters (and Lines) before the command **renumerate** is invoked are 5, 17, and 23. The numbers after are 10, 20, and 30.

```
OS900(script-IpInterface01)# show

script 'IpInterface01' : Play Dome at Tensa.
                  Parameters
---- -------------- -------------- -----------
Num. Name           Type           Description
---- -------------- -------------- -----------
   5 vifID          vifN           Param for interface ID.
  17 portID         ports          Group of Ports
  23 tagID          tag            ID of Tag
OS900(script-IpInterface01)# renumerate
OS900(script-IpInterface01)# show

script 'IpInterface01' : Play Dome at Tensa.
                  Parameters
---- -------------- -------------- -----------
Num. Name           Type           Description
---- -------------- -------------- -----------
  10 vifID          vifN         Param for interface ID.
  20 portID         ports          Group of Ports.
  30 tagID          tag            ID of Tag.
```

## Lines

Lines are a sequence of CLI commands that include script Parameters.

The actions that can be performed on a *line* are as follows:

- Create Line
- View Line
- Modify Line
- Delete Line

**Create Line**

To create a line:

1. Enter **`configure terminal`** mode.
2. Enter the mode of a script (existing or new) by invoking the command:
   **`script NAME`**
   where,
   **`NAME`**: Name of script. String of up to thirteen alphanumeric characters. Letter characters must be lowercase only and must not be blanks, e.g., **`ipiface01`**.
3. Invoke the command:
   **`line [NUMBER] COMMAND`**
   where,
   **`NUMBER`**: (optional) Number for the line.
   **`COMMAND`**: CLI command in the regular format with the exception that instead of a value argument, a parameter preceded by **`$`** is entered.

Example

```
OS900# configure terminal
OS900(config)# script ipiface01
OS900(script-ipiface01)# line      10   interface vlan vif$IFID
OS900(script-ipiface01)#
```

| | |
|---|---|
| | **Note**<br>When creating a script, there is no need to use **`exit`** command in order to return to previous CLI modes. |

**View Line**

The procedures for viewing a Line are the same as those given for viewing a Script – see section *Viewing*, page *122*.

**Modify Line**

To modify a line re-enter it with the same line number as follows:

1. Enter the mode of the script containing the line to be modified by invoking the command:
   **`script NAME`**
   where,
   **`NAME`**: Name of script.
2. Invoke the command:
   **`line NUMBER COMMAND`**
   where,
   **`NUMBER`**: Number for the line.
   **`COMMAND`**: New CLI command.

**Delete Line**

To delete a line from an existing script:

1. Enter **`configure terminal`** mode.
2. Enter the mode of the script containing the line to be deleted by invoking the command:

**script NAME**

where,

**NAME**: Name of script.

3. Invoke the command:

   **no line NUMBER**

   where,

   **NUMBER**: Number of the line to be deleted.

Example

```
OS900(script-ipiface01)# no line 50
OS900(script-ipiface01)#
```

### Renumber Lines

To renumber all Lines (and Parameters) of a script with the sequence 10, 20, 30, etc.:

1. Enter the mode of the script by invoking the command:

   **script NAME**

   where,

   **NAME**: Name of script.
2. Renumber the Lines (and Parameters) by invoking the command:

   **renumerate**

Example

The example below shows that the numbers of the Lines (and Parameters) before the command **renumerate** is invoked are 5, 17, and 23. The numbers after are 10, 20, and 30.

```
OS900(script-IpInterface01)# show

script 'IpInterface01' : Play Dome at Tensa.
                  Parameters
---- -------------- -------------- -----------
Num. Name           Type           Description
---- -------------- -------------- -----------
   5 vifID          vifN         Param for interface ID.
  17 portID         ports          Group of Ports
  23 tagID          tag            ID of Tag
OS900(script-IpInterface01)# renumerate
OS900(script-IpInterface01)# show

script 'IpInterface01' : Play Dome at Tensa.
                  Parameters
---- -------------- -------------- -----------
Num. Name           Type           Description
---- -------------- -------------- -----------
  10 vifID          vifN         Param for interface ID.
  20 portID         ports          Group of Ports.
  30 tagID          tag            ID of Tag.
OS900(script-IpInterface01)#
```

## Viewing

### In Script Mode

To view a script in its mode:

1. Enter **configure terminal** mode.
2. Enter the mode of the script whose parameters are to be viewed by invoking the command:

   **script NAME**

   where,

   **NAME**: Name of script.
3. Invoke the command:

   **show**

Example

```
OS900# configure terminal
OS900(config)# script ipiface01
OS900(script-ipiface01)# show

script 'ipiface01'
                  Parameters
---- -------------- -------------- -----------
Num. Name           Type           Description
---- -------------- -------------- -----------
  10 IFID           ifname         Vlan Interface ID
  20 POID           ports          Group of Ports
  30 TGID           tag            ID of Tag
  40 IPID           ipv4_pref      IP Prefix of Interface

                  Lines
---- -----------------------------------------
Num. Line
---- -----------------------------------------
  10 interface vlan vif$IFID
  20  ports $POID
  30  tag $TGID
  40  ip $IPID
OS900(script-ipiface01)#
```

**In Enable Mode**

To view one or all scripts in **enable** mode:

***One Script***

1. Enter **enable** mode.
2. Invoke the command:
   **show script NAME**
   where,
   **NAME**: Name of script.

***All Scripts***

1. Enter **enable** mode.
2. Invoke the command:
   **show scripts [configuration]**
   where,
   **configuration**: (optional) In the format used to configure the parameters. If this keyword is not entered, the parameters are displayed in tabular format.

## Executing

A Script can be executed like any other CLI command.
To execute a script

1. Enter **enable** mode.
2. Invoke the command:
   **NAME**
   where,
   **NAME**: Name of script.
3. Press Shift ? to display the parameter value to be entered, and enter the value prompted by the system.
4. Repeat step *3*, above, until the prompt <cr> appears.

## Deleting

To delete a script:

1. Enter **`configure terminal`** mode.
2. To display the list of existing scripts, type the partial command:
   **`no script ?`**
3. Complete the partial command by typing the name of the script to be deleted.

Example

```
OS900# configure terminal
OS900(config)# no script ?
  NAME
  Config07       *Script*
  IpInterface01  *Script* Play Dome at Tensa.
OS900(config)# no script Config07
OS900(config)#
```

## Example

The example below shows how a script is created that can be used to configure an interface. Custom entries are shown in the color `red`. Parameter names are in upper case, e.g., IFID, POID, TGID. Notice that in each line, a regular CLI command (e.g., **`tag 27`**) is entered with the exception that a parameter (e.g., **`TGID`**) preceded by **`$`** is entered instead of a value (e.g., **`27`**).

```
MRV OptiSwitch 910 version d1734-22-09-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
OS900(config)# script ?
  NAME  Script name

OS900(config)# script ipiface01

OS900(script-ipiface01)# parameter 10   IFID type vifN description Vlan Interface ID
OS900(script-ipiface01)# parameter 20   POID type ports description Group of Ports
OS900(script-ipiface01)# parameter 30   TGID type tag description ID of Tag
OS900(script-ipiface01)# parameter 40   IPID type ipv4_pref description IP Prefix of
Interface
OS900(script-ipiface01)# line      10   interface vlan vif$IFID
OS900(script-ipiface01)# line      20   _ports $POID
OS900(script-ipiface01)# line      30   _tag $TGID
OS900(script-ipiface01)# line      40   _ip $IPID

OS900(script-ipiface01)# show
script 'ipiface01'
                  Parameters
---- -------------- -------------- -----------
Num. Name           Type           Description
---- -------------- -------------- -----------
  10 IFID           vifN           Vlan Interface ID
  20 POID           ports          Group of Ports
  30 TGID           tag            ID of Tag
  40 IPID           ipv4_pref      IP Prefix of Interface

                  Lines
---- -----------------------------------------
Num. Line
---- -----------------------------------------
  10 interface vlan vif$IFID
  20  ports $POID
  30  tag $TGID
  40  ip $IPID
```

```
OS900(script-ipiface01)# exit
OS900(config)# exit
OS900# ipiface01 ?
  <1-4095>  Vlan Interface ID
OS900# ipiface01 201 ?
  PORT_GROUP_STR  Group of Ports
OS900# ipiface01 201 2-4 ?
  <1-4095>  ID of Tag
OS900# ipiface01 201 2-4 2001 ?
  A.B.C.D/M  IP Prefix of Interface
OS900# ipiface01 201 2-4 2001 192.4.4.4/24 ?
  <cr>
  |     Output modifiers
OS900# ipiface01 201 2-4 2001 192.4.4.4/24
Interface is activated.
vty execute: 'interface vlan vif201'
vty execute: ' ports 2-4'
vty execute: ' tag 2001'
vty execute: ' ip 192.4.4.4/24'
OS900#
```

# Console Access Control

## Disabling the Console

Local access to the OS900 [via the out-of-band RS-232 interface (***CONSOLE EIA-232*** port)] for management can be disabled.

| ⚠ | **CAUTION!** Before disabling local access to the OS900, ensure that a TELNET or SSH connection exists, otherwise the OS900 will be locked to access! |
|---|---|

To disable local access to the OS900, from the *remote* management station:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`console-disable [delayed]`**

   where,

   **`delayed`**: Delay access disabling for one minute

## Enabling the Console

To enable local access to the OS900 [via the out-of-band RS-232 interface] a TELNET or SSH connection is required to have existed at the time local access was disabled.

To re-enable local access to the OS900, invoke the command:

**`no console-disable`**

# Layer 2 Protocol Counters

Several counters, one for each of Layer 2 protocols, count the number of ingress and egress frames separately. These counters can be viewed and cleared.

## Viewing

To view the Layer 2 protocol counters, invoke the command:

**`show l2cntrl-protocol-counters`**

Example

```
OS900# show l2cntrl-protocol-counters
PROTOCOL      TX_COUNTER  RX_COUNTER
------------------------------------
 L2CNTRL_STP       5          38
 L2CNTRL_OAM       0          0
```

```
 L2CNTRL_EFM       0          0
 DOT1X             0          0
 LACP              0          0
 DOT1AH            0          0
 UDLD              0          0
 CDP               0          0
 PVST              0          0
 VTP               0          0
OS900#
```

The fields in the above example are described below.

| | |
|---|---|
| `L2CNTRL_STP` | IEEE 802.1s (MSTP) and IEEE 802.1w (RSTP) protocols |
| `L2CNTRL_OAM` | IEEE 802.1ag and ITU-T SG Y.1731 Ethernet Service OAM protocols |
| `L2CNTRL_EFM` | IEEE 802.3ah OAM for Ethernet in the First Mile protocol |
| `DOT1X` | IEEE 802.1x Wireless LAN authentication protocol |
| `LACP` | IEEE 802.3ad Link Aggregation/Trunking protocol |
| `DOT1AH` | IEEE 802.1ah Provider Bridged Networks interconnection protocol |
| `TX_COUNTER` | *Egress* frames counter |
| `RX_COUNTER` | *Ingress* frames counter |

### Clearing

To clear all the Layer 2 protocol counters, invoke the command:

**`clear l2cntrl-protocol-counters`**

Example

```
OS900# clear l2cntrl-protocol-counters
OS900#
```

## Default Configuration

This section applies only for OS900s especially configured for customers who have specifically asked for setup with the default configuration of the OS900.

### Viewing

To view the default configuration of the OS900:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`show default-configuration`**

### Setting

To set the default configuration for the OS900:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`write default-configuration`**

# Chapter 6: Ports

## General

This chapter shows how to configure and monitor the physical ports of the OS900.

## Enabling/Disabling

### Default

By default, each data (customer) port is *enabled*.

### Custom

Each port can be enabled or disabled independently of other ports. To enable/disable one or more ports, invoke the following command:

**`port state enable|disable PORTS-GROUP|all`**

where,

**`port`**: Port-related action

**`state`**: Port state

**`enable`**: Enable the port(s)

**`disable`**: Disable the port(s)

**`PORTS-GROUP`**: Group of Ports. (The ports can be members of a trunk.)

**`all`**: All ports

Example

```
OS900(config)# port state disable 4
port 4 state set to: DISABLE
OS900(config)#
```

## Status

### Brief

To view the configuration status of one or more ports in *brief*, invoke the command:

**`show port [PORTS-GROUP|all]`**

where,

**`show`**: Display

**`port`**: Port-related action

**`[PORTS-GROUP]`**: Group of Ports.
(If no port number is entered, the statuses of all ports are displayed.)

**`all`**: All ports

Example

```
OS910(config)# show port
PORTS CONFIGURATION
===================
PORT MEDIA      MEDIA_SEL LINK  SPD_SEL     LAN_SPD   DUPL  STATE     SL
---------------------------------------------------------------------
1    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
2    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
3    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
4    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
5    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
6    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
7    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE    1
8    TP         COPPER    ON    AUTO         1 GBps   FULL  ENABLE    1
t1   ---         ---      ON    AUTO         2 GBps   FULL  ENABLE    1
(9)  SFP+100FX  SFP       ON-F  AUTO         1 GBps   FULL  ENABLE    1
(10) SFP+100FX  SFP       ON-F  AUTO         1 GBps   FULL  ENABLE    1
OS910(config)#
```

## Detailed

To view the configuration status of one or more ports in *detail*, invoke the command:

**`show port details [PORTS-GROUP]`**

where,

**`show`**: Display

**`port`**: Port-related action

**`details`**: Detailed information

**`[PORTS-GROUP]`**: Group of Ports
(If no port number is entered, the statuses of all ports are displayed.)

Example

```
OS904-DSL4# show port details 1
Port 1 details:
-------------------
Description          : Port 1 - ETH10/100/1000
Type                 : ETH10/100/1000
Media-select mode    : AUTO
Link                 : ON (15h29m12s)
Duplex state         : N/A
PHY                  : COMBO+100FX
Speed selected       : AUTO
Auto-Neg Advertise   : Default
Selected cross mode  : AUTO
Bypass mode          : ENABLE
State                : ENABLE
Priority             : 1
Flow control mode    : off
Ethertype            : CORE1:0x8100
OutBound Tagged      : untagged
UDLD Protocol        : -

OS904-DSL4#
```

# Comment Adding

To enter a textual description of one or more ports, invoke the command:

**`port description PORTS-GROUP|all ..`**

where,

**`port`**: Port-related action

**`description`**: Textual description

**PORTS-GROUP**: Group of Ports

**all**: All ports

`..`: Textual description to be entered

Example

```
OS900(config)# port description 4 This port is for new customers.
OS900(config)# show port details 4
Port 4 details:
-------------------
Description       : This port is for new customers.
Type              : ETH100/1000
Media-select mode : SFP
Link              : OFF
Duplex state      : N/A
PHY               : SFP+100FX
Speed selected    : AUTO
Auto-Neg Advertise: Default.
Bypass mode       : ENABLE
State             : ENABLE
Priority          : 1
Flow control mode : off
Ethertype         : CORE1:0x8100
OutBound Tagged   : untagged
Tags List         :

OS900(config)#
```

# Physical Interface

## Default

After booting, the OS900 will check if a 100Base-FX SFP is present at a port and if so it will automatically set the physical interface to 100Base-X, i.e., to the argument value **sfp100** in the command **port media-select**. The command is described in the section *Custom*, below.

If the SFP is not a 100Base-FX SFP, by default, the type of physical interface selected for an SFP port is **sfp** (1000Base-X).

## Custom

The type of physical interface for an SFP port can be selected independently of other ports. To select the interface medium for one or more ports, invoke the following command:

**port media-select sfp|sfp100|copper|auto PORT-GROUP|all**

where,

**port**: Port-related action

**media-select**: Port physical interface

**sfp**: Set the port to operate as a 1000Base-X interface (default)

**sfp100**: Set the port to operate as a 100Base-X interface

**copper**: Set the port to operate with the fixed 10/100/1000Base-T interface

**auto**: Set the port to operate with the SFP or fixed 10/100/1000Base-T interface automatically

**PORT-GROUP**: Group of Ports

**all**: All ports

Example

```
OS900(config)# port media-select copper 1,2
port 1 media mode set to: COPPER
port 2 media mode set to: COPPER
OS900(config)
```

### Viewing

To view the type of physical interface set for ports, invoke the command **`show port details PORT-GROUP`** as described in the section *Brief*, page *127*.

## MDI/MDIX

### Default

By default, the port interface is automatically configured to function as MDI or MDIX so that the port can communicate via its co-port. (Default)

To set one or more ports in the default mode, invoke the command:

**`no port crossover-mode (PORTS-GROUP|all)`**

**`PORTS-GROUP`**: Group of Ports

**`all`**: All ports

### Custom

To set the interface of one or more ports in the default, MDI, or MDIX mode, invoke the command:

**`port crossover-mode (mdi|mdix|auto) (PORTS-GROUP|all)`**

where,

**`mdi`**: MDI configuration of port interface

**`mdix`**: MDIX configuration of port interface

**`auto`**: Automatic MDI or MDIX configuration of port interface – in order for the port to communicate via its co-port. (Default)

**`PORTS-GROUP`**: Group of Ports

**`all`**: All ports

## Speed

### Default

The default speed of an electrical data (customer) port is according to *auto-negotiation*. (data ports are shown in *Figure 2*, page *65*.)

### Custom

The speed of each port can be set (forced) independently of other ports. To set a speed for one or more ports, invoke the following command:

**`port speed 10|100|1000|auto PORTS-GROUP|all`**

where,

**`port`**: Port-related action

**`speed`**: Speed to be set

**`10`**: 10 Mbit/sec (Applicable to 10/100/1000Base-T ports only)

**`100`**: 100 Mbit/sec

**`1000`**: 1000 Mbit/sec

**`auto`**: Auto-Negotiation

**`PORTS-GROUP`**: Group of Ports

**`all`**: All ports

Example

```
OS900(config)# port speed 1000 1,2
port 1 speed set to: FORC1,000
port 2 speed set to: FORC1,000
OS900(config)#
```

### Viewing

To view the speed configurations for ports, invoke a **show** command as described in the section *Status*, page *127*.

## Link Mode (Bypass)

### Default

By default, the two ports at the end of a link, even if one is set for auto-negotiation speed while the other is set for a fixed speed, are enabled.
To set one or more ports in the default mode, invoke the command:

**port bypass (PORTS-GROUP|all)**

where,

**PORTS-GROUP**: Group of Ports

**all**: All ports

### Custom

To cause the link between two ports to remain broken so long as one port is set for auto-negotiation speed while the other is set for a fixed speed, invoke the command:

**no port bypass (PORT-GROUP|all)**

**PORTS-GROUP**: Group of Ports

**all**: All ports

### Viewing

To view the link mode for ports, invoke a **show** command as described in the section *Status*, page *127*.

## Duplexity

### Default

The default duplexity mode of transmission of a 10/100/1000Base-T data port is according to *auto-negotiation*.

### Custom

The duplexity of each port can be set (forced) independently of other ports. To set half- or full-duplexity for one or more ports, invoke the following command:

**port duplex half|full PORTS-GROUP|all**

where,

**port**: Port-related action

**duplex**: Duplexity to be set

**half**: Half-duplex

**full**: Full-duplex

**PORTS-GROUP**: Group of Ports

**all**: All ports

Example

```
OS900(config)# port duplex half 1,2
port 1 duplex set to: HALF
port 2 duplex set to: HALF
OS900(config)#
```

### Viewing

To view the speed configurations for ports, invoke a **`show`** command as described in the section *Status*, page *127*.

# Traffic Throughput Reading

### For User-specified Time Interval

To view the rate of traffic flow through one or more ports in a user-specified time interval, invoke the command:

**`show port rate (PORTS-GROUP|all) time (<10-60>)`**

**`PORTS-GROUP`**: Group of ports for which the traffic throughput is to be measured.

**`all`**: All ports' traffic throughput is to be measured.

**`(<10-60>)`**: Time interval during which the throughput is to be measured. The measurement starts as soon as the command is invoked.

<u>Example</u>

```
OS910# show port rate 1,3 time 15

The answer will be ready in 15 more seconds
OS910#
Results for port 1:
Tx: 511 Kbps, 999 pps, rate 0.671 Mbps
Rx: 511 Kbps, 1998 pps, rate 0.831 Mbps

Results for port 3:
Tx: 511 Kbps, 999 pps, rate 0.671 Mbps
Rx: 511 Kbps, 1998 pps, rate 0.831 Mbps

OS910# show port rate 1,3 time 10
The answer will be ready in 10 more seconds
OS910#
Results for port 1:
Tx: 511 Kbps, 998 pps, rate 0.671 Mbps
Rx: 511 Kbps, 1997 pps, rate 0.830 Mbps

Results for port 3:
Tx: 511 Kbps, 998 pps, rate 0.671 Mbps
Rx: 511 Kbps, 1997 pps, rate 0.830 Mbps
OS910#
```

In the example above, `Kbps` is kilo*bits* per second, `pps` is packets per second, and `Mbps` is mega*bits* per second. The rates in KBps and pps apply to Layer 2. The rate in Mbps applies to Layer 1.

### Of Last User-specified Time Interval

To view the amount of traffic that flowed through one or more ports in the last user-specified time interval, invoke the command:

**`show port rate PORTS-GROUP|all`**

**`PORTS-GROUP`**: Group of ports for which the traffic throughput is to be measured.

**`all`**: All ports' traffic throughput is to be measured.

Example

```
OS910# show port rate 1,3

Results for port 1:
Tx: 511 KBps, 998 pps, rate 0.671 Mbps
Rx: 511 KBps, 1997 pps, rate 0.830 Mbps
Measures were taken at: Wed Jul 30 10:31:56 2008

Results for port 3:
Tx: 511 KBps, 998 pps, rate 0.671 Mbps
Rx: 511 KBps, 1997 pps, rate 0.830 Mbps
Measures were taken at: Wed Jul 30 10:31:56 2008
OS910#
```

### Of Latest User-specified Time Intervals

To view the amount of traffic that flowed through one or more ports in the last user-specified time intervals (up to five), invoke the command:

**show port rate (PORTS-GROUP|all) time (<10-60>)**

**PORTS-GROUP**: Group of ports for which the traffic throughput is to be measured.

**all**: All ports' traffic throughput is to be measured.

**(<10-60>)**: Time interval during which the throughput is to be measured.

Example

```
OS910# show port rate 1,3 history

Rate results for port 1:
-------------- at: Wed Jul 30 10:37:38 2008 --------------
Tx: 511 KBps, 998 pps, rate 0.671 Mbps
Rx: 511 KBps, 1997 pps, rate 0.830 Mbps
-------------- at: Wed Jul 30 10:37:24 2008 --------------
Tx: 511 KBps, 999 pps, rate 0.671 Mbps
Rx: 511 KBps, 1998 pps, rate 0.831 Mbps

Rate results for port 3:
-------------- at: Wed Jul 30 10:37:38 2008 --------------
Tx: 511 KBps, 998 pps, rate 0.671 Mbps
Rx: 511 KBps, 1997 pps, rate 0.830 Mbps
-------------- at: Wed Jul 30 10:37:24 2008 --------------
Tx: 511 KBps, 999 pps, rate 0.671 Mbps
Rx: 511 KBps, 1998 pps, rate 0.831 Mbps
OS910#
```

To view the last result use:
**show port rate (PORTS-GROUP|all)**

To view the history of the last 5 results:
**show port rate (PORTS-GROUP|all) history**

# Port SFP Reading

### Parameters

To view the SFP port internal EEPROM data, invoke the command:

**show port sfp-params [PORTS-GROUP]**

**sfp-params**: SFP port internal EEPROM data.

**PORTS-GROUP**: Group of ports for which the traffic throughput is to be measured. Trunk ports may be included.

Example

```
OS910# show port sfp-params t1

 SFP ports internal EEPROM data
================================

   Trunk t1, Port 9: SFP EEPROM Parameters
 **************************************************************************
  Identifier is SFP
  Connector code is LC
  Transceiver subcode is 1000Base-SX
  Serial encoding mechanism is 8B10B
  The nominal bit rate is 1300 Megabits/sec.
  Link length using single mode (9 micron) is not supported.
  Link length using 50 micron multi-mode fiber is greater than 500m.
  Link length using 62.5 micron multi-mode fiber is greater than 300m.
  Link length using copper cable is not supported.
  Vendor name is Infineon AG
  Vendor PN is V23818-K305-B57
  Vendor revision is 1
  Vendor SN is 30355175
  Nominal transmitter output wavelength at room temperature is not specified.
 **************************************************************************


   Trunk t1, Port 10: SFP EEPROM Parameters
 **************************************************************************
  Identifier is SFP
  Connector code is LC
  Transceiver subcode is 1000Base-SX
  Serial encoding mechanism is 8B10B
  The nominal bit rate is 2100 Megabits/sec.
  Link length using single mode (9 micron) is not supported.
  Link length using 50 micron multi-mode fiber is greater than 300m.
  Link length using 62.5 micron multi-mode fiber is greater than 150m.
  Link length using copper cable is not supported.
  Vendor name is MRV
  Vendor PN is SFP-DGD-SX
  Vendor revision is A
  Vendor SN is PDL16FH
  Nominal transmitter output wavelength at room temperature is 850.00 nm.
 **************************************************************************
```

## Diagnostics

To view the digital diagnostics of the SFP's internal EEPROM, invoke the command:

**`show port sfp-diag [PORTS-GROUP]`**

**`sfp-diag`**: Digital diagnostics of the SFP's internal EEPROM.

**`PORTS-GROUP`**: Group of ports for which the traffic throughput is to be measured. Trunk ports may be included.

Example

```
OS910# show port sfp-diag t1

 SFP ports internal EEPROM data
================================
 Trunk t1, Port 9: Digital Diagnostic feature is not supported for current SFP

   Trunk t1, Port 10: SFP Digital Diagnostics
 ****************************************************
  Description           Real-Time Value
  --------------------  ---------------
  Temperature (C)/(F):    47/116
  Voltage         (V):     3.3248
  TX Bias        (mA):     7.408
  TX Power (dBm)/(mW):   -4.7/0.337
  RX Power (dBm)/(mW):   -5.2/0.303
 ****************************************************
OS910#
```

# Capabilities Advertising

## General

*Port capabilities advertising* is the advertising of the speed(s) and duplexity with which ports can operate.

## Applicability

*Port capabilities advertising* applies only to 10/100/1000Base-T ports.

## Requirement

For ports to be able to advertise they must be set in auto-negotiation mode. One or more ports can be set in auto-negotiation mode by invoking the command **`port speed auto PORTS-GROUP|all`** described in the section *Speed*, page *130*.

## Default

The default advertise mode for ports is advertise all speeds (10, 100, and 1000 Mbps) and both duplexities (half and full) that the ports are capable of.

## Custom

### Advertising a Speed and Duplexity

To set one or more ports to advertise a speed and duplexity (and possibly other speeds and the other duplexity) that the ports are capable of, invoke the following command:

**`port advertise speed (10|100|1000|all) duplex (half|full|all) (PORTS-GROUP|all)`**

where,

**`port`**: Port-related action

**`advertise`**: Advertise default auto-negotiation capabilities

**`speed`**: Speed to be set

**`10`**: 10 Mbit/sec (Applicable to 10/100/1000Base-T ports only)

**`100`**: 100 Mbit/sec

**`1000`**: 1000 Mbit/sec

**`all`**: (First appearance) All speeds (10, 100, and 1000 Mbit/sec)

**`duplex`**: Duplexity to be set

**`half`**: Half-duplex

**`full`**: Full-duplex

**`all`**: (Second appearance) Both duplexities (half and full)

**`PORTS-GROUP`**: Group of Ports

**`all`**: (Third appearance) All ports

By repeated use of the above command the ports can be set to advertise their other speeds and their other duplexity that they are capable of.

Note that this command will cause the port to advertise:

– The speed specified in the command, in addition to one or more other set speeds (if they exist for the port), and

– The duplexity specified in the command, in addition to the other set duplexity (if it exists for the port)

Example

```
OS910(config)# port advertise speed 100 duplex half 3,5
port 3 advertise set to speed: 100MBps, duplex: HALF
port 5 advertise set to speed: 100MBps, duplex: HALF
OS910(config)#
```

**Default**

To set one or more ports in the default advertising mode (described in the section *Default*, page *135*), invoke the command:

**`port advertise default (PORTS-GROUP|all)`**

where,

**`PORTS-GROUP`**: Group of Ports

**`all`**: All ports

**Preventing All Advertising**

To prevent one or more ports from advertising, invoke the command:

**`no port advertise default (PORTS-GROUP|all)`**

where,

**`PORTS-GROUP`**: Group of Ports

**`all`**: All ports

**Preventing Advertising of a Speed and Duplexity**

To prevent one or more ports from advertising a specific speed and duplexity, invoke the command:

**`no port advertise speed (10|100|1000|all) duplex (half|full|all) (PORTS-GROUP|all)`**

where,

**`10`**: 10 Mbit/sec (Applicable to 10/100/1000Base-T ports only)

**`100`**: 100 Mbit/sec

**`1000`**: 1000 Mbit/sec

**`all`**: (First appearance) All speeds (10, 100, and 1000 Mbit/sec)

**`half`**: Half-duplex

**`full`**: Full-duplex

**`all`**: (Second appearance) Both duplexities (half and full)

**`PORTS-GROUP`**: Group of Ports

**`all`**: (Third appearance) All ports

**Advertising *only* a Specific Speed and Duplexity**

To set one or more ports to advertise *only* a specific speed and duplexity, and no other. This is done by invoking the command in the section *Preventing Advertising of a Speed and Duplexity*, page *136*, for each speed and duplexity that is to be excluded.

For example, to set 10/100/1000Base-T ports 1 and 2 to advertise *only* the speed *100 Mbps* and the duplexity *Half*:

1. Prevent all advertising by ports 1 and 2 by invoking the command:
   **`no port advertise 1,2`**
2. Enable advertising by ports 1 and 2 of speed *100 Mbps* and duplexity *Half* by invoking the command:
   **`port advertise speed 100 duplex half 1,2`**

### Viewing

To view the speed configurations for ports, invoke a **`show`** command as described in the section *Status*, page *127*.

## Outbound Tag Mode

To change the outbound tag mode for a port after an ACL has been bound to a port, unbind the ACL (as described in the section *Unbinding*, page *318*, change the outbound tag mode (as described below), then rebind the ACL (as described in the section *Binding*, page *316*).

One or more ports can be set to handle ingress frames with IEEE 802.1Q encapsulation in one of the following modes:

- Tagged
- Untagged
- Hybrid
- Q-in-Q

### Tagged

To set a port to handle *only* tagged ingress frames[14] (and to forward them with the tag):

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port tag-outbound-mode tagged PORTS-GROUP`**
   where,
   **`port`**: Port-related action
   **`tag-outbound-mode`**: IEEE 802.1Q encapsulation of ingress/egress frames
   **`tagged`**: Tagged ingress/egress frames
   **`PORTS-GROUP`**: Group of Ports
   (If no port number is entered, all ports are selected.)

### Untagged

This is the default mode for ports. To set a port to handle only untagged ingress frames (and to forward them untaggged):

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port tag-outbound-mode untagged PORTS-GROUP`**
   where,
   **`port`**: Port-related action
   **`tag-outbound-mode`**: IEEE 802.1Q encapsulation of ingress/egress frames
   **`untagged`**: Untagged ingress/egress frames
   **`PORTS-GROUP`**: Group of Ports
   (If no port number is entered, all ports are selected.)

[14] Untagged ingress frames are dropped in tagged mode.

## Hybrid

This mode is similar to tagged mode except for the way it handles untagged frames. In tagged mode, ingress untagged frames are dropped. In hybrid mode, ingress untagged frames are assigned the port's default tag. Egress packets having the default tag are sent untagged.

To configure hybrid mode for a group of ports:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port tag-outbound-mode hybrid [PORTS-GROUP] TAG`**

   where,

   **`port`**: Port action

   **`tag-outbound-mode`**: IEEE 802.1Q encapsulation of ingress/egress frames

   **`hybrid`**: Tagged and untagged ingress/egress frames

   **`[PORTS-GROUP]`**: Group of Ports
   (If no port number is entered, all ports are selected.)

   **`TAG`**: User-selectable default tag for the interface

## Q-in-Q (Service VLAN Access Mode)

The Q-in-Q mode is used to interconnect customer sites having *the same* VLAN tag across an Ethernet metro network.

This mode applies for *access* (LAN) ports. In this mode both tagged and untagged frames are allowed at ingress. All ingress frames are encapsulated with an additional tag (Service VLAN tag). All egress frames at tagged ports are stripped of Service VLAN tags.

To configure Q-in-Q mode for one or more access ports:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port tag-outbound-mode q-in-q [PORTS-GROUP] TAG`**

   where,

   **`port`**: Port configuration.

   **`tag-outbound-mode`**: IEEE 802.1Q encapsulation of ingress/egress frames

   **`q-in-q`**: Untagging of ingress/egress frames. This argument must be selected for Q-in-Q *access* ports.

   **`[PORTS-GROUP]`**: Group of Ports
   (If no port number is entered, all ports are selected.)

   **`TAG`**: Default Service VLAN tag to be added to a packet that enters any of the ports in the **`PORTS-GROUP`**.

   This tag can be swapped using an ACL rule. For details, refer to the section *Stage 2 – Actions on Packet*, page *304*.

## Viewing

To view the tags of one or more ports:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`show port tag [PORT-GROUP|all]`**

   where,

   **`[PORT-GROUP]`**: Group of Ports
   (If no port number is entered, all ports are displayed.)

   **`all`**: All ports

Example

```
OS910M# show port tag 1-3
Value of ethertype 1 is 0x8100 (default value)
Value of ethertype 2 is 0x8100 (default value)

PORT TAG CONFIGURATION
======================
port   OUTBOUND-TAGGED DEF-TAG NUM-TAGS ETHERTYPE     TAGS-LIST
------------------------------------------------------------------------------
1      tagged             0      1     CORE1:0x8100  10
2      tagged             0      1     CORE1:0x8100  10
3      tagged             0      1     CORE1:0x8100  10
OS910M#
```

The `NUM-TAGS` column shows the number of VLAN interfaces of which a port is a member.

`DEF-TAG` is the tag that will be assigned to untagged frames entering the port.

# Multi-VLAN Membership for Untagged Ports

Normally, an untagged port can be a member of only one VLAN. However, by enabling such a port for multi-VLAN membership, the port will know how to direct each ingress packet to the right VLAN.

To configure a group of multi-VLAN untagged ports:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port untagged-multi-vlans PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Group of untagged ports to be members in several VLANs.
3. For each multi-VLAN untagged port/group, configure an ACL (see ***Chapter 15:*** *Extended Access Lists (ACLs)*, page *295*) that specifies the VLAN to which a packet type entering the port/group is to be sent. Then bind the ACL to each of the multi-VLAN untagged ports/groups.

# Link Protection

The Link Protection (dual-homing) mechanism is used to set two links to backup each other. When the primary link fails, the backup (secondary) link takes over the tasks of the primary link, and vice versa.

Three examples are given below to serve as guides in configuring Link Protection.

## Example 1 – Using Two Devices

### Network

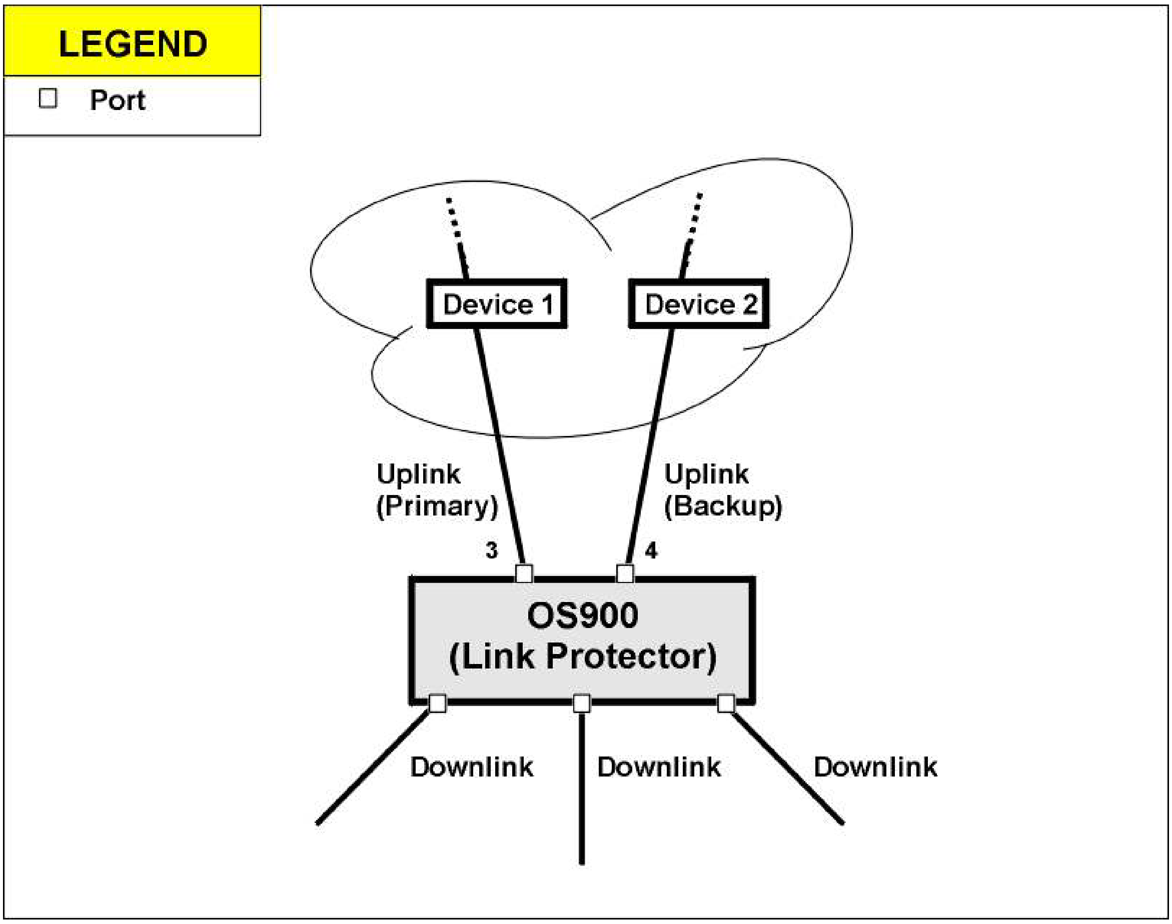



**Figure 14: Link Protection Data Path using Two Devices**

### Enabling

To enable Link Protection using two devices, invoke the command:

**`link-protection primary PORT backup PORT [no-preemption]`**

where,

**`PORT`**: (*First* appearance) Primary Port number.

**`PORT`**: (*Second* appearance) Backup Port number.

**`no-preemption`**: Prevent the primary port from retaking over from the backup port when it recovers.

### Implementation

```
OS910(config)# port trunk t1 3,4
OS910(config)# 3 backup 4
OS910(config)# link-protection primary 3 backup 4
OS910(config)#
```

## Example 2 –Using a Single Remote IEEE 802.1ag MEP

**Network**

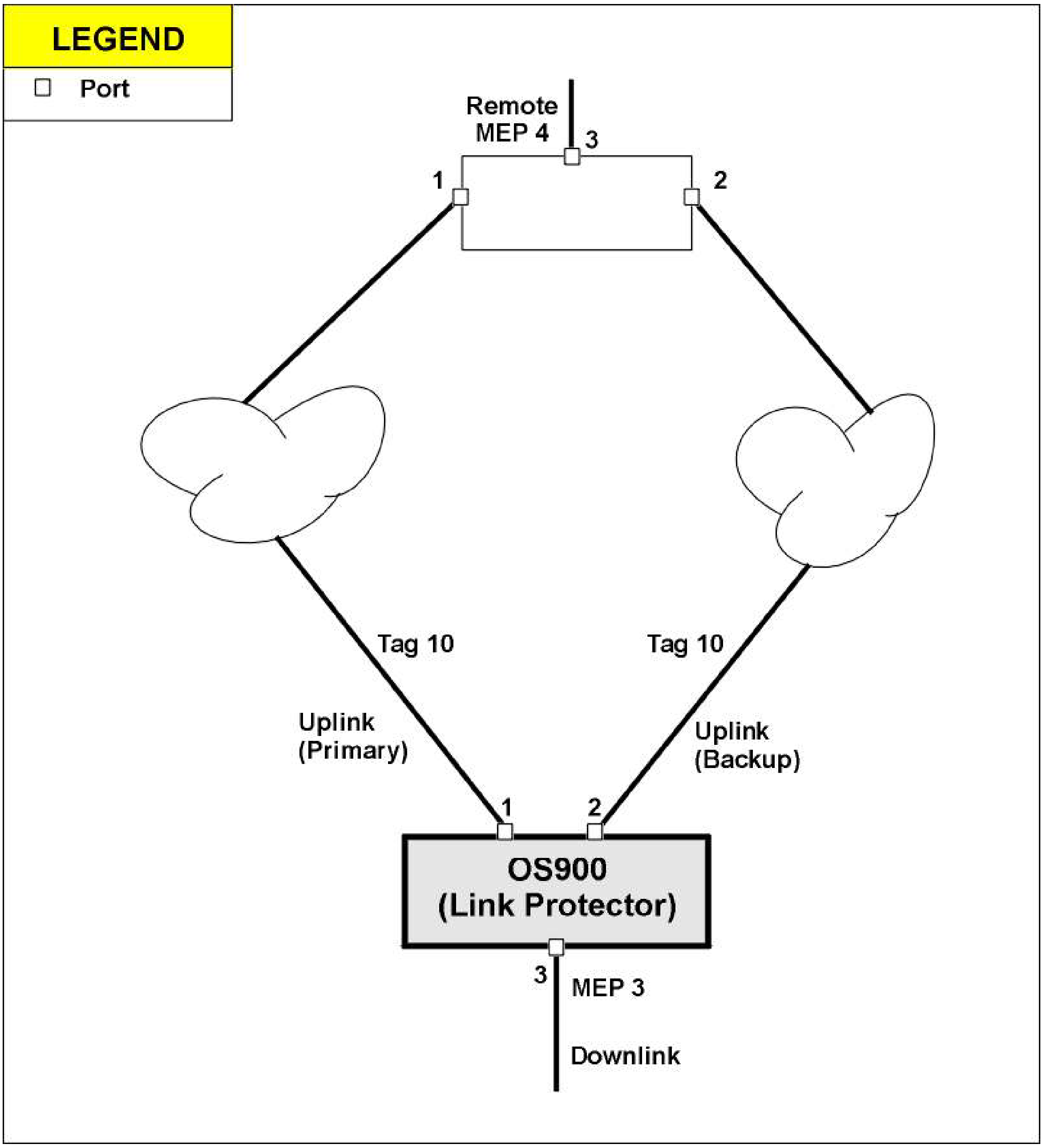



**Figure 15: Link Protection Data Path using a Single Remote MEP in an IEEE 802.1ag-configured Network**

**Enabling**

To enable Link Protection using a single remote MEP, invoke the command:

```
link-protection primary PORT backup PORT srv NUMBER dmn <0-7> [rmep <1-4095>]
```

where,

**PORT**: (*First* appearance) Primary Port number.

**PORT**: (*Second* appearance) Backup Port number.

**NUMBER**: IEEE 802.1ag Service ID value.

**<0-7>**: IEEE 802.1ag domain level value (range **0..7**).

**[rmep <1-4095>]**: Remote MEP ID in the range **<1..4095>**.

**Note**

When links are connected to a MEP, the Link-Protection mechanism operates only in the **`no-preemption`** mode.

### Implementation

```
-------------------------------------------------Configuring Link Protector-------------------------------------------------
!
hostname LINK_PROT_DEV
!
port trunk t1 1-2
!
link-protection primary 1 backup 2 srv 1 dmn 2 rmep 4
!
interface vlan vif10
 tag 10
 ports 3,t1
!
ethernet oam domain 2
  service 1
    vlans 10
    remote-meps 4
    mep 3 port 3
    mep 3 activate
    mep 3 ccm-activate
!
ethernet oam enable
!
----------------------------------------Configuring Device with Remote MEP 4----------------------------------------
!
hostname MEP-4
!
interface vlan vif10
 tag 10
 ports 1-3
!
ethernet oam domain 2
  service 1
    vlans 10
    remote-meps 3
    mep 4 port 3
    mep 4 activate
    mep 4 ccm-activate
!
ethernet oam enable
```

**Link Protection Data Path using Dual Remote IEEE 802.1ag MEPs**

**Network**

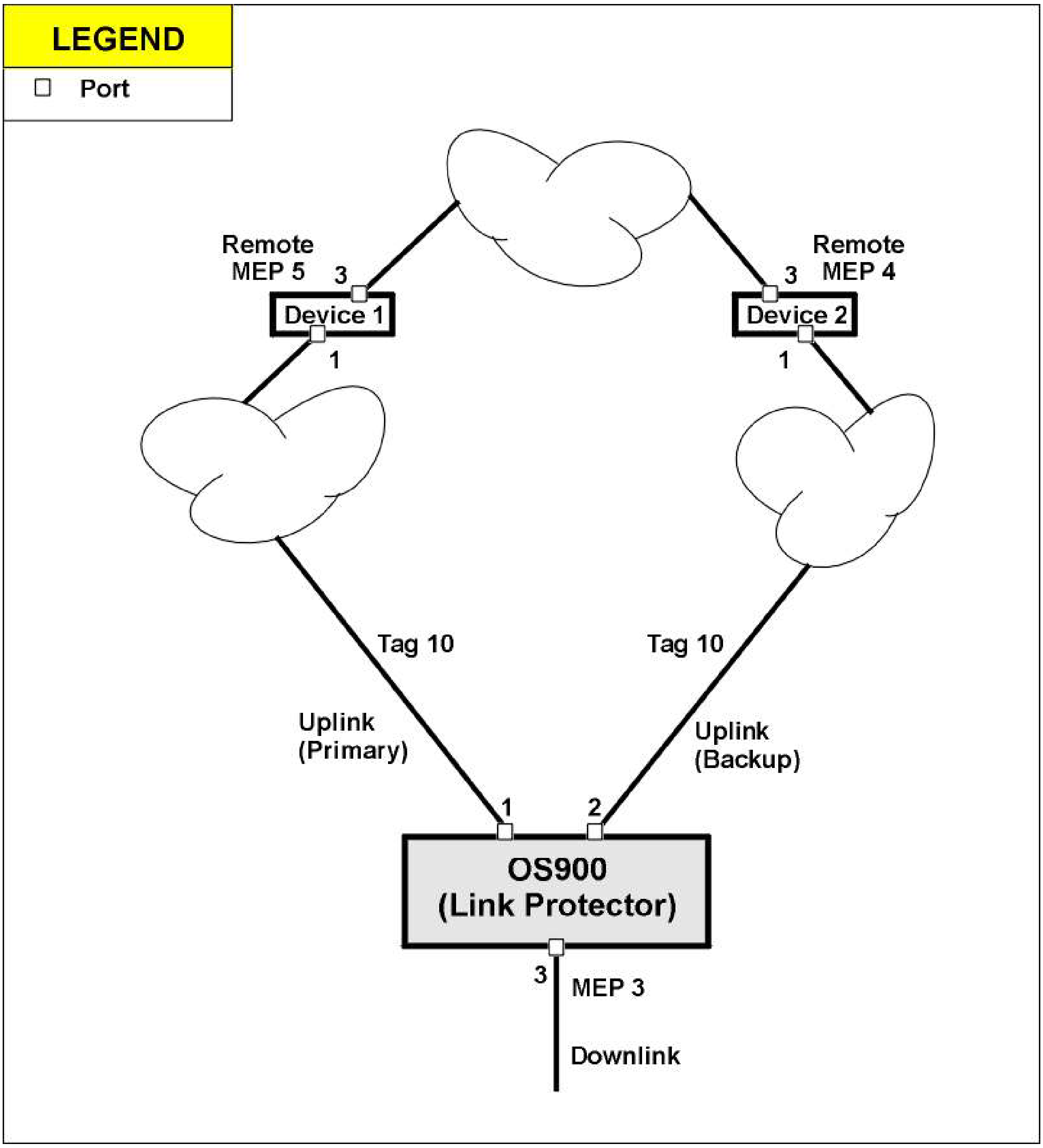



**Figure 16: Link Protection Data Path using Dual Remote MEPs in an IEEE 802.1ag-configured Network**

### Enabling

To enable Link Protection using dual remote MEPs, invoke the command:

```
link-protection primary PORT rmep <0-7> SRV_NUMBER <1-4095> backup
PORT rmep <0-7> SRV_NUMBER <1-4095>
```

where,

`PORT`: (*First* appearance) Port number of Primary Link.

`<0-7>`: (*First* appearance) Domain level value of Primary Remote MEP (range `0..7`).

`SRV_NUMBER`: (*First* appearance) Service ID of Primary Remote MEP.

`<1-4095>`: (*First* appearance) Primary MEP ID (range `<1..4095>`.

`PORT`: (*Second* appearance) Port number of Backup Link.

**<0-7>**: (*Second* appearance) Domain level value of Backup Remote MEP (range **0..7**).

**SRV_NUMBER**: (*Second* appearance) Service ID of Backup Remote MEP.

**<1-4095>**: (*Second* appearance) Backup MEP ID (range **<1..4095>**.

| | Note |
|---|---|
| | When links are connected to a MEP, the Link-Protection mechanism operates only in the **no-preemption** mode. |

### Implementation

```
------------------------------------------------Configuring Link Protector------------------------------------------------

hostname LINK_PROT_DEV
!
port trunk t1 1-2
!
link-protection primary 1 rmep 2 1 4 backup 2 rmep 2 1 5
!
interface vlan vif10
 tag 10
 ports 3,t1
!
ethernet oam domain 2
  service 1
    vlans 10
    remote-meps 4-5
    mep 3 port 3
    mep 3 activate
    mep 3 ccm-activate
!
ethernet oam enable
!
---------------------------------------Configuring Device with Remote MEP 4---------------------------------------

hostname MEP-4
!
interface vlan vif10
 tag 10
 ports 1,3
!
ethernet oam domain 2
  service 1
    vlans 10
    remote-meps 3
    mep 4 port 3
    mep 4 activate
    mep 4 ccm-activate
!
ethernet oam enable
!

---------------------------------------Configuring Device with Remote MEP 5---------------------------------------
hostname MEP-5
!
interface vlan vif10
 tag 10
 ports 1,3
!
```

```
ethernet oam domain 2
  service 1
    vlans 10
    remote-meps 3
    mep 5 port 3
    mep 5 activate
    mep 5 ccm-activate
!
ethernet oam enable
!
```

## Disabling

To disable Link Protection:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no link-protection primary PORT**

   where,

   **PORT**: Primary Port number.

Example

```
OS910(config)# no link-protection primary 3
OS910(config)#
```

## Viewing

To view the link-protection status invoke the command:

1. Enter **enable** mode.
2. Invoke the command:

   **show port details [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports whose link-protection status is to be viewed.

Example

```
OS904# show port details t1
Trunk t1 details:
-------------------
Description                : N/A
Link                       : OFF
Duplex state               : N/A
Speed selected             : AUTO
Auto-Neg Advertise         : Default
Selected cross mode        : AUTO
Bypass mode                : ENABLE
State                      : ENABLE
Priority                   : 1
Flow control mode          : off
Ethertype                  : CORE1:0x8100
OutBound Tagged            : untagged
Tags List                  :
Udld                       : -
Link-protection            : primary 3 and backup 4 with preemption. Now active is 4.
OS904#
```

## Changing the Primary Link Port

This section applies if the two ports were set in link-protection mode *without* preemption.

To change the Primary Link port:

1. Enter **configure terminal** mode.
2. Invoke the command:

```
link-protection primary PORT active PORT
```

where,

| | |
|---|---|
| **PORT** | (First appearance) Old (existing) Primary Port number. |
| **PORT** | (Second appearance) New Primary Port number. |

Example

```
OS900(config)# link-protection primary 4 active 3
OS900(config)#
```

# Link Reflection

The Link Reflection /Propagation or Link Integrity Notification (LIN) mechanism provides notification on the integrity of a link from the NNI to the UNI even if the link extends through *several* OS900s. It allows terminal equipment to detect link failure in the path between two terminal equipment units. The link failure is propagated throughout the network until it reaches the remote OS900, which disables the transmission immediately upon failure detection.

Referring to *Figure 17*, below, the Link Reflection mechanism downs the link at the downlink ports (that are assigned to the uplink port) if the link at the uplink port fails.

Using the Link Reflection mechanism, two OS900s interconnected *across a network* can be configured so that if the link to a UNI at *one* OS900 goes down, the link to the corresponding UNI at the *other* OS900 is automatically brought down – see *Figure 18*, page *148*.

| **Note** |
|---|
| If the uplink port is a trunk, Link Reflection is activated only if all ports of the trunk fail. |

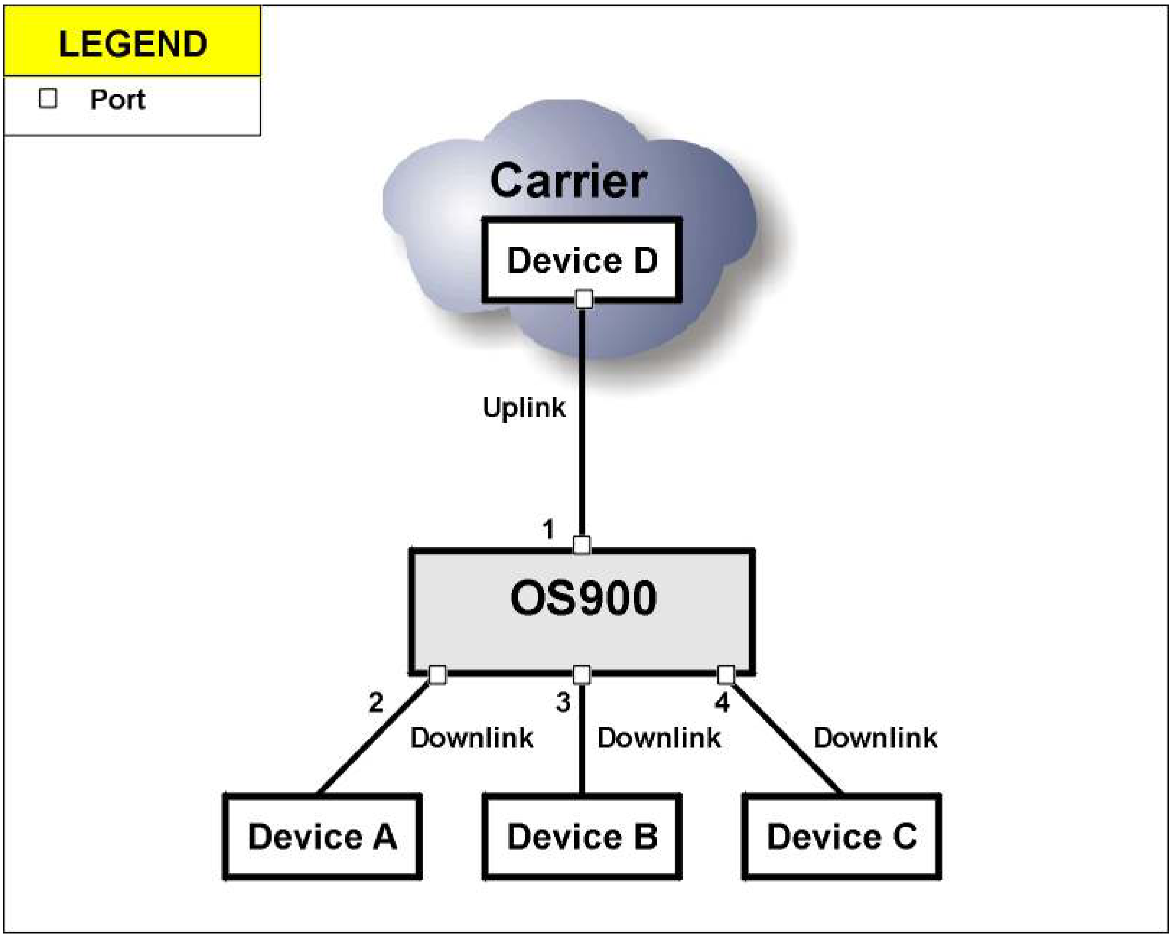



**Figure 17: Link Reflection between Uplink and Downlink**

## Enabling

To enable Link Reflection:

1. Enter **configure terminal** mode.
2. Invoke any of the following commands:

    **link-reflection uplink PORT downlink PORTS-GROUP**

    or

    **link-reflection uplink PORT downlink PORT symmetrical**

    or

    **link-reflection uplink PORT downlink PORTS-GROUP srv NUMBER dmn <0-7> [rmep <1-4095>]**

    where,

    **PORT**: (First appearance) Uplink (usually core or provider network) port number.

    **PORT**: (Second appearance) Downlink access port number.

    **symmetrical**: Down the link at the uplink port if the link at the downlink port fails. (This option can be applied provided only one port is specified as the downlink port. In such a case, Link Reflection can function for both the uplink and downlink port.)

    **PORTS-GROUP**: Downlink access port numbers.

    **srv NUMBER**: IEEE 802.1ag Service ID value.

    **dmn <0-7>**: IEEE 802.1ag domain level value (range **0..7**).

    **[rmep <1-4095>]**: Remote MEP ID in the range 1-4095. Default: If there is only one remote MEP, it is not required to specify the remote MEP ID.

Example 1

```
OS910(config)# link-reflection uplink 1 downlink 2-4
OS910(config)#
```

Example 2

The following example shows Link Reflection configuration with Ethernet Service OAM for two OS900s interconnected across a network. In this configuration, if the link to a UNI at *one* OS900 is broken, the link to the corresponding UNI at the *other* OS900 is also broken.

*Network*

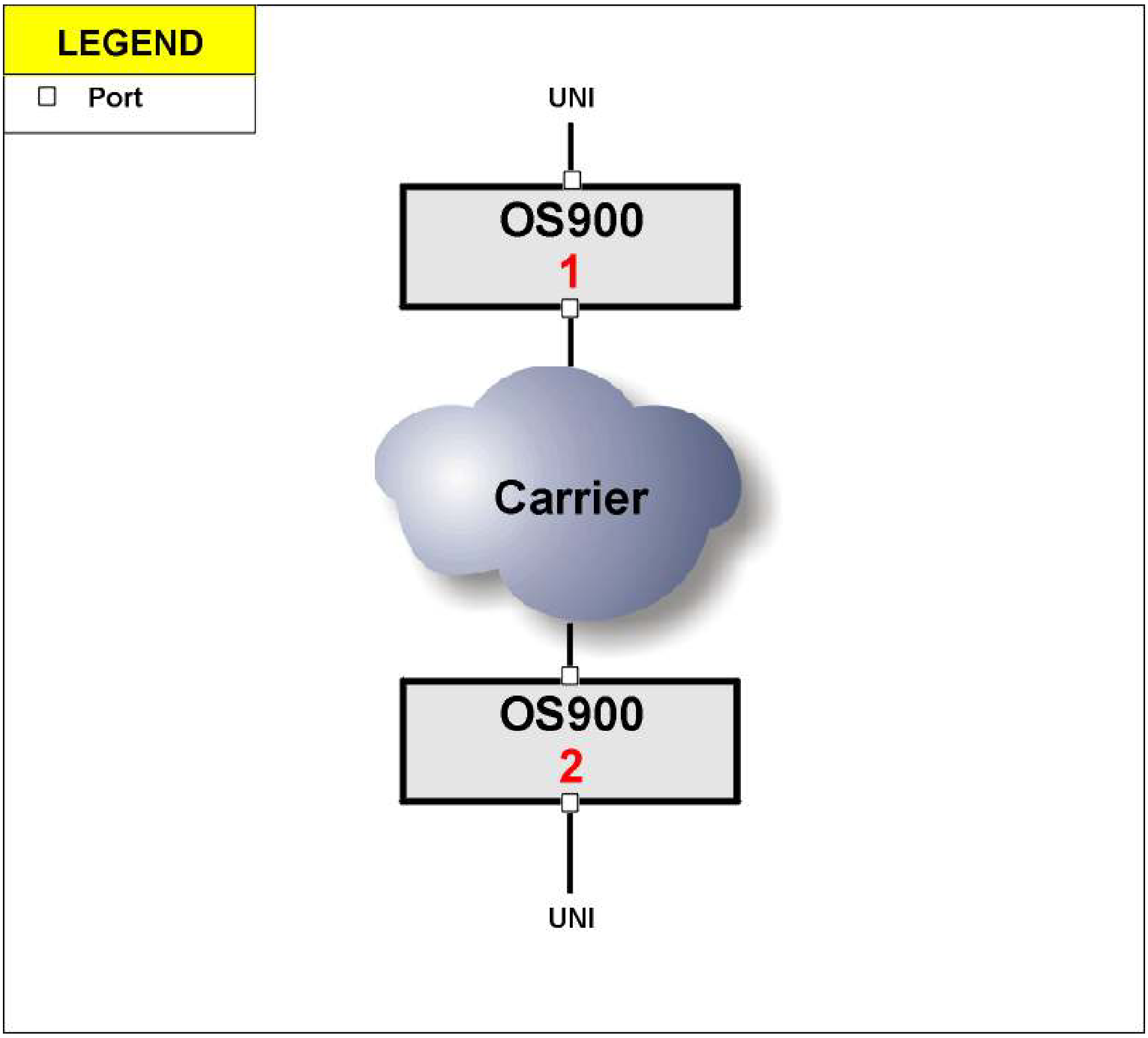



**Figure 18: Link Reflection between Two UNIs**

*Configuration*

Following are the CLI commands for implementing Link Reflection between two OS900s across the network shown in *Figure 18*, above.

When a port is dependent only upon the remote MEP, invoke the command **`link-reflection uplink PORT srv NUMBER dmn <0-7>`** to enable link reflection.

```
OS900 1

link-reflection uplink 1 srv 1 dmn 1
!
interface vlan vif10
 tag 10
 ports 1,4
!
ethernet oam domain 1
  service 1
    primary-vlan 10
    vlans 10
    remote-meps 1
    mep 2 port 1
    mep 2 activate
    mep 2 ccm-activate
!
```

```
ethernet oam enable


OS900 2

link-reflection uplink 1 srv 1 dmn 1
!
interface vlan vif10
 tag 10
 ports 1,4
!
ethernet oam domain 1
  service 1
    primary-vlan 10
    vlans 10
    remote-meps 2
    mep 1 port 1
    mep 1 activate
    mep 1 ccm-activate
!
ethernet oam enable
```

### Disabling

To disable Link Reflection:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no link-reflection uplink PORT**
   where,
   **PORT**: Uplink-port number.

Example

```
OS900(config)# no link-reflection uplink 1
OS900(config)#
```

### Viewing

To view whether link reflection is enabled or disabled:

1. Enter **enable** mode.
2. Invoke the command:
   **show link-reflection**

Example

```
OS900# show link-reflection
Link-Reflection Table
---------------------------------------------------------------------------
Uplink Port: Downlink Ports                  : Options
---------------------------------------------------------------------------
 1         : 1                              : domain 1 service 1
OS900#
```

## Port Protection (Private VLAN)

### Definition

Port protection is the creation of one or more private (edge) VLANs within an existing VLAN.

### Purpose

Port protection is used to direct traffic entering a VLAN to user-selected egress ports in the VLAN.

## Advantage

In an Ethernet network, port protection provides additional security to hosts on the same subnet by isolating the ports (from one another) to which they are connected even if the ports are members of the same VLAN.

## Configuration

This mechanism directs traffic at one group of user-selectable source (ingress) ports to another group of user-selectable destination (egress) ports, all ports being members of the same VLAN.

To enable Port Protection:

1. Enter **configure terminal** mode.
2. Invoke the command:

    **port protected PORTS_GROUP|all allowed-dst PORTS_GROUP**

    where,

    **protected**: Egress traffic restriction.

    **PORTS_GROUP**: (First appearance) Group of source ports.

    **allowed-dst**: Allow traffic to destination ports.

    **PORTS_GROUP**: (Second appearance) Group of destination ports.

Example

```
OS900(config)# port protected 1,2 allowed-dst 3,4
OS900(config)#
```

## Viewing

To view the destination ports to which traffic from the associated source ports is restricted:

1. Enter **enable** mode.
2. Invoke the command:

    **show port protected [PORTS_GROUP]**

    where,

    **[PORTS_GROUP]**: Group of source ports.

Example

```
OS900# show port protected 1-4
  Port protected:
 -----------------
source port   destination ports
    1            3-4
    2            3-4
    3            all
    4            all
OS900#
```

# Link Flap Guard

## General

Link Flap Guard is a mechanism that isolates a port that changes its link state with an unacceptably high frequency.

By default, the Link Flap Guard is disabled.

## Custom Setting

In the *default* setting, the Link Flap Guard is disabled.

To set a link flap frequency at which ports are to be isolated:

1. Enter **configure terminal** mode.
2. Invoke the command:

**link-flap guard <5-10000> port (PORTS-GROUP|all)**

where,

**<5-10000>**: Link flap frequency (i.e., number of changes per second in the link state of a port) for which a port is to be isolated

**PORTS-GROUP**: Group of ports to have the link flap frequency apply

**all**: All ports to have the link flap frequency apply

Example

```
OS900(config)# link-flap guard 1257 port 2-4
OS900(config)#
```

## Viewing

To view the setting of the Link Flap Guard:

1. Enter **enable** mode
2. Invoke the command:

**show link-flap guard port (PORTS-GROUP|all)**

**PORTS-GROUP**: Group of ports for whom the setting of the Link Flap Guard is to be viewed

**all**: All ports to have the setting of the Link Flap Guard for them viewed

Example

```
OS900# show link-flap guard port 2-4
Link Flap Guard
----------------------
Port   Guard Threshold
----------------------
2      1257
3      1257
4      1257
OS900#
```

## Default Setting

To set the link flap guard to the default setting, i.e., to disable it:

1. Enter **configure terminal** mode.
2. Invoke either of the following commands:

**link-flap guard default port (PORTS-GROUP|all)**

**no link-flap guard port (PORTS-GROUP|all)**

Example

```
OS904(config)# link-flap guard default port 3
Link flap guard mechanism has been disabled for port(s) 3.
OS904(config)#
```

## Reconnecting Isolated Ports

To reconnect one or more ports that have been isolated:

1. Enter **configure terminal** mode.
2. Invoke the command:

**port state enable PORTS-GROUP|all**.

where,

**PORTS-GROUP**: Group of ports to be recovered. (The ports can be members of a trunk.)

**all**: All ports to be recovered.

Example

```
OS910(config)# port state enable 2,3
port 2 state set to: ENABLE
port 3 state set to: ENABLE
OS910(config)#
```

# Link Flap Dampening

## General

Link Flap Dampening is a mechanism that can be used to *temporarily* isolate one or more ports that change their link state with an unacceptably high frequency.

## Principle of Operation

The flapping port is assigned a **`flap-penalty`** for each flap. Once the total of the accumulated flap penalties reaches the **`errdisable-threshold`** the port is isolated. If now the port link stops flapping, for each passing link flap interval[15] the total of the accumulated penalties is decreased by the **`stability-grant`** value. When the total drops to zero the port will be allowed to reconnect to the network provided it is set to recover. By default, the port is preset to recover when the Link Flap Dampening mechanism is enabled, as described below. (In any case, the port can be set/preset to recover using the command **`port errdisable recover cause link-flap PORTS-GROUP`**.) If the port is isolated a second time, the **`errdisable-threshold`** is automatically doubled. If the port is isolated a third time, the **`errdisable-threshold`** is automatically tripled. And so on. If the port is enabled using the command **`port state enable|disable PORTS-GROUP|all`**, the user-set **`errdisable-threshold`** value is reestablished.

## Parameters Setting

### Penalty per Flap

The Penalty per Flap is a number assigned to a flap. The larger the number, the larger is the penalty.

To set the penalty value per flap:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`link-flap-dampening flap-penalty VALUE`**

   where,

   **`VALUE`**: Flap penalty value

Example

```
OS910(config)# link-flap-dampening flap-penalty 5
OS910(config)#
```

### Threshold for Port Isolation

The Threshold for Port Isolation is the product of the flap penalty value and the number of link flaps.

To set the value of the threshold:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`link-flap-dampening errdisable-threshold VALUE`**

   where,

   **`VALUE`**: Threshold value for port isolation

[15] The link flap interval is displayed when the command **`show link-flap-dampening`** is invoked, as described in the section *Configuration*, page *153*.

Example

```
OS910(config)# link-flap-dampening errdisable-threshold 40
OS910(config)#
```

### Stability Grant

The Stability Grant is a number by which the total of the accumulated penalties is decremented for each minute that no flap occurs since isolation. If no flap occurs until the accumulated penalties for a port are decremented to zero, the port can reconnect to the network provided it is allowed to be recoverable. The section *Recovering Isolated Ports*, page *155*, shows how to make ports recoverable.

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`link-flap-dampening stability-grant VALUE`**
   where,
   **`VALUE`**: Flap penalty value

Example

```
OS910(config)# link-flap-dampening stability-grant 8
OS910(config)#
```

## Enabling

To enable the Link Flap Dampening mechanism:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port errdisable detect cause link-flap PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Group of ports to be *handled by* the Link Flap Dampening mechanism

Example

```
OS910(config)# port errdisable detect cause link-flap 1,4
OS910(config)#
```

## Disabling

To disable the Link Flap Dampening mechanism:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`no port errdisable detect cause link-flap PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Group of ports to be *freed of* the Link Flap Dampening mechanism

Example

```
OS910(config)# no port errdisable detect cause link-flap 4
OS910(config)#
```

## Viewing

### Configuration

To view the Link Flap Dampening configuration

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show link-flap-dampening`**

Example

```
OS910# show link-flap-dampening
Link-flap dampening configuration:
   Errdisable threshold = 10
   Flap penalty         = 1
   Stability grant      = 2
   Interval             = 60 seconds
OS910#
```

### Operation Data

#### *Brief*

To view the Link Flap Dampening operation data *in brief*:

1. Enter **enable** mode.
2. Invoke the command:
   **show port link-flap-dampening PORTS-GROUP**
   where,
   **PORTS-GROUP**: Group of ports to be *freed of* the Link Flap Dampening mechanism

Example

```
OS910# show port link-flap-dampening 1,4
PORT   DETECT  RECOVERY PENALTY FLAPS-CNT ERRDIS-CNT RECOVER-CNT STATE
========================================================================
1      ENABLE  ENABLE        0         0          0           0  ENABLE
4      ENABLE  ENABLE        0         0          0           0  ENABLE
OS910#
```

#### *Detailed*

To view the Link Flap Dampening operation data *in detail*:

1. Enter **enable** mode.
2. Invoke the command:
   **show port link-flap-dampening long PORTS-GROUP**
   where,
   **long**: Detailed information
   **PORTS-GROUP**: Group of ports to be *freed of* the Link Flap Dampening mechanism

Example

```
OS910# show port link-flap-dampening long 1,4
Port 1
===========
Port state is ENABLE
Link flap dampening is enabled
Recovery from errdisable state is enabled
The current penalty is 0
The total number of link flaps is 0
The port never entered errdisable state
The port never recovered from errdisable state
Port 4
===========
Port state is ENABLE
Link flap dampening is enabled
Recovery from errdisable state is enabled
The current penalty is 0
The total number of link flaps is 0
The port never entered errdisable state
The port never recovered from errdisable state
OS910#
```

## Recovering Isolated Ports

By default, ports are preset to be recoverable (i.e., allowed to reconnect to the network) when the Link Flap Dampening mechanism is enabled.

To recover isolated ports when the total of the accumulated penalties drops to zero:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port errdisable recover cause link-flap PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports to be *allowed* by the Link Flap Dampening mechanism

Example

```
OS910(config)# port errdisable recovery cause link-flap 3
OS910(config)#
```

# Regular, Dual, and Extra Internal Ports

## General

OS900 models have regular ports, dual ports, or extra internal ports. A regular port consists of one external port. An external port is physically accessible. A dual port consists of one external port and one internal port. An internal port is physically inaccessible. An extra internal port is an internal port that can be flexibly assigned to a regular port or to a dual port.

**Table 9: Regular, Dual, and Extra Internal Ports**

| Model | Ports | | |
|---|---|---|---|
| | Regular | Dual | Extra Internal |
| OS904 | – | 1 to 4 | e1 |
| OS906 | – | 1 to 6 | e1 to e9 |
| OS910, OS910-M | – | 1 to 10 | e1 to e3 |
| OS912 | 11, 12 | 1 to 10 | – |
| OS930 | 2, 3 | 1 | – |

In the user manual, the internal ports are distinguished from the external ports only where required. In CLI commands, internal ports are identified by the keyword **extra**.

## Application

The dual-port feature provides for:

– Configuring a *dual* leaky-bucket policer (instead of a *single* leaky-bucket policer) as described in the section *Dual Leaky-Bucket Policer*, page *367*.

– Tag translation as described in ***Chapter 12:*** *Tag Translation/Swapping*, page *265*.

– Setting of separate flood rates for up to two different traffic types for the same ingress port as described in the section *Configuration*, page *249*.

– Ingress shaping of traffic as described in the section *Hierarchical QoS*, page *292*.

## Bypassing Internal Ports

As a rule, the default (factory-set) setting for internal ports *should not be changed*. In the default setting, internal ports are *not* bypassed. Before changing the default setting, it is advisable to consult MRV's CSO.

To bypass all the internal ports:

1. Enter **boot** mode.
2. Invoke the command:
   **no internal-ports**

Example

```
OS900(config)# boot
OS900(config-boot)# no internal-ports
Action will come into effect after rebooting
OS900(config-boot)#
```

### Revoking Bypass of Internal Ports

To revoke bypassing of internal ports:

1. Enter **boot** mode.
2. Invoke the command:
   **internal-ports**

Example

```
OS900(config)# boot
OS900(config-boot)# internal-ports
Action will come into effect after rebooting
OS900(config-boot)#
```

# Double Tagging Mode

### General

Physical ports of an OS900 can be configured to double-tag packets entering it from the user side.

### Requirement

Ports to be double-tagged must be dual ports (described in the section *Regular, Dual, and Extra Internal* Ports, page *155*).

### Principle of Operation

Packets entering a port configured to double-tag from the *user* side are stripped of *all* their tags, if present, tagged with the two user-preselected VLAN tags, and switched to the network side.

Packets entering a port configured to double-tag from the *network* side are stripped of their *two* user-preselected VLAN tags and forwarded untagged to the user side.

*Figure 19*, below, is a schematic illustrating the process.

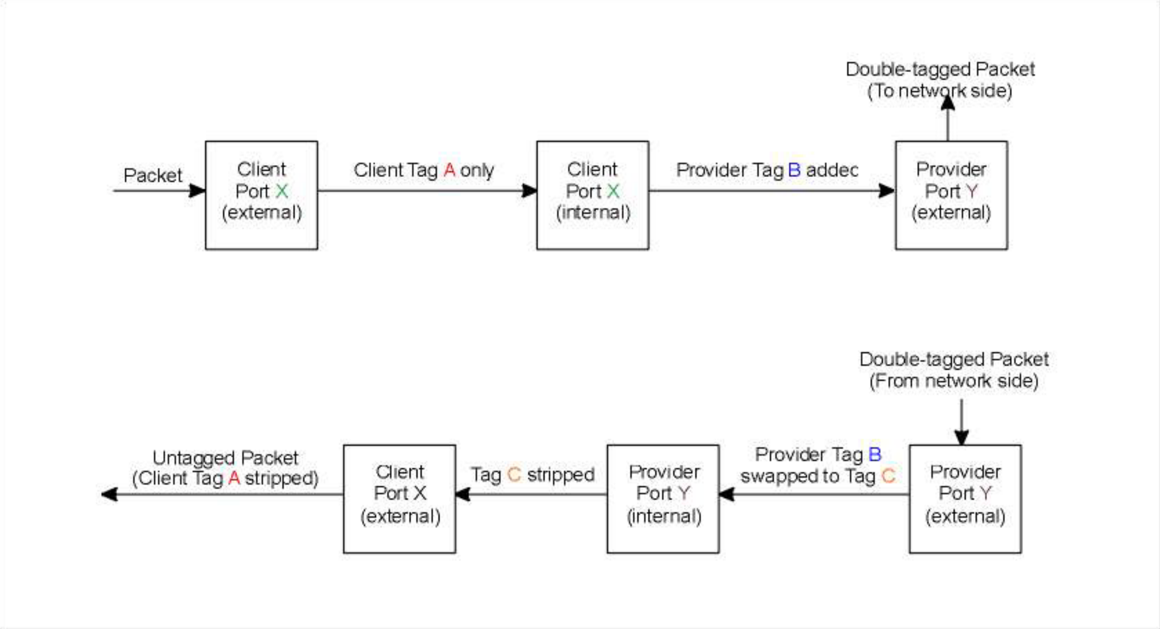



**Figure 19: Double Tagging Process**

## Implementation

In the following implementation, the *provider* port is Port 4 and the *client* ports, set to double-tag packets, are Ports 1 to3. One of the double tags is the client tag (10, 20, or 30), the other tag is the provider tag (100).

In order for the double tags

```
---------------------------Adding provider tag 100 to packets that have client tag 10, 20, or 30---------------------------

Building configuration...

Current configuration:
! version 2_1_4
!
access-list extended port1_extra
 rule 10
  action tag nest 100
  tag eq 10
!
access-list extended port2_extra
 rule 10
  action tag nest 100
  tag eq 20
!
access-list extended port3_extra
 rule 10
  action tag nest 100
  tag eq 30
!

---------------------------------------------Swapping provider tag 100 with tag 999---------------------------------------------

access-list extended port4_strip
 rule 10
  action tag swap 999
  tag eq 100
!
```

-----------------------------Assigning a textual description to the client and provider ports-----------------------------

```
port description 1 Customer1
port description 2 Customer2
port description 3 Customer3
port description 4 NetworkPort
```

--------------------------Forcing traffic entering ports 1-3 from client side via provider port 5--------------------------

```
port protected 1-3 allowed-dst 4
!
```

-------------Adding client tag to packets from client side and deleting tag from packets to client side-------------

```
port tag-outbound-mode q-in-q 1 10
port tag-outbound-mode q-in-q 2 20
port tag-outbound-mode q-in-q 3 30
```

----Adding provider tag to packets entering port 4 from client side, stripping tag from packets to client side----

```
port tag-outbound-mode hybrid 4 999
!
```

------------------------------------Binding ACLs to the provider and internal client ports------------------------------------

```
port acl-binding-mode by-port 1-3
port access-group port4_strip 4
port access-group extra port1_extra 1
port access-group extra port2_extra 2
port access-group extra port3_extra 3
!
```

----------------------Creating VLAN interfaces, each including the client port and provider port----------------------

```
interface vlan vif10
 tag 10
 ports 1,4
!
interface vlan vif20
 tag 20
 ports 2,4
!
interface vlan vif30
 tag 30
 ports 3,4
!
interface vlan vif100
 tag 100
 ports 1-4
!
interface vlan vif999
 tag 999
 ports 4
!
```

-----------------------------Enabling remote management via the out-of-band Ethernet port-----------------------------

```
interface out-of-band eth0
 ip 10.90.136.74/24
```

```
 management
!

-------------Disabling learning of MAC addresses of stations whose traffic is received by the OS900-------------

no lt learning
!
```

# Loopback at Layer 2

Layer 2 frames received at a group of ports can be looped back to their sources. This is done by swapping their source address with their destination address.

## Enabling

A port can operate in loopback mode, provided it is not a member of a VLAN to which an ACL is bound! To enable a group of ports to operate in loopback mode:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port layer2-loopback PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports *to swap* source and destination addresses

Example

```
OS904(config)# port layer2-loopback 2-4
OS904(config)#
```

## Disabling

To disable a group of ports from operating in loopback mode:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no port layer2-loopback [PORTS-GROUP]**

   where,

   **PORTS-GROUP**: Group of ports *not to swap* source and destination addresses

Example

```
OS904(config)# no port layer2-loopback 2-4
OS904(config)#
```

# Flow Control

## Definition

Flow Control is a mechanism that causes a transmitting station to temporarily backoff when the port memory of the OS900 becomes saturated.

## Purpose

Flow Control is used to prevent packet-loss. It is to be invoked when it is preferable to lower the transmission rate rather than have packets dropped due to congestion.

## Applicability

Flow control can be applied *per-port* to full-duplex ports.

It cannot be applied to trunk ports.

### Effect

Flow control may impact SLA, such as bandwidth and QoS.

### Principle of Operation

Flow Control is set up between the OS900 and a transmitting station on a point-to-point link. Whenever the OS900 becomes congested, it sends back a "pause" frame to the transmitting station at the other end of the link, instructing it to stop sending packets for a pre-specified time period. The transmitting station waits during the requested time period before transmitting again.

### Configuration

#### Enabling

To enable Flow Control:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port flow-control PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Numbers of physical ports for which flow control is to be *enabled*

#### Disabling

To disable Flow Control:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`no port flow-control PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Numbers of physical ports for which flow control is to be *disabled*

#### Viewing

To view whether Flow Control is enabled or disabled for a port:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show port details [PORTS-GROUP]`**
   where,
   **`PORTS-GROUP`**: Group of physical ports

### Compliance

IEEE 802.3x flow control protocol for full-duplex ports.

# Statistics

## Viewing

#### Momentary

##### *Brief*

To view the *momentary* statistical information (brief) on one or more ports (possibly a port trunk) in tabular format:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show port statistics table [PORTS-GROUP]`**
   where,

**PORTS-GROUP**: Group of ports. For a port trunk the format is **tX**, where, **X** is a numerical. Example **t3**.

Example

```
OS900# show port statistics table

PO SEND       SEND      SEND       RECV       RECV      RECV       RECV
NO UNI        BROAD     MULTI      UNI        BROAD     MULTI      ERR
=============================================================================
1  0          0         157198     0          0         0          0
2  0          0         0          0          0         0          0
5  0          0         0          0          0         0          0
6  0          0         0          0          0         78582      0
7  0          0         157198     0          0         0          0
8  0          0         0          0          0         0          0
9  0          0         0          0          0         0          0
10 0          0         0          0          0         0          0
t1 0          0         0          0          0         0          0
OS900#
```

***Detailed***

To view the *momentary* statistical information (detailed) on one or more ports (possibly a port trunk):

1. Enter **enable** mode.
2. Invoke the command:
   **show port statistics PORTS-GROUP**
   where,
   **PORTS-GROUP**: Group of ports. For a port trunk the format is **tX**, where, **X** is a numerical. Example **t3**.

Example

```
OS900# show port statistics t1

PORTS STATISTICS
================

Port t1 Ethernet counters
---------------------------
Good bytes received                    : 249980170703
Good packets received                  : 3905937622
Good unicast packets received          : 3905934745
Good broadcast packets received        : 0
Good multicast packets received        : 2877
Bytes transmitted                      : 250013089300
Packets transmitted                    : 3906453227
Unicast packets transmitted            : 3906451771
Broadcast packets transmitted          : 1456
Multicast packets transmitted          : 0
CRC or Alignment error received        : 2
Undersize received                     : 0
Oversize received                      : 0
Fragments received                     : 1
Jabber received                        : 0
Collisions received and transmitted    : 0

Port t1 RMON Packet Size Distribution Counters
------------------------------------------------
    -  64 Octets : 7812379774
  65- 127 Octets : 4338
 128- 255 Octets : 0
 256- 511 Octets : 0
```

```
 512-1023 Octets : 0
1024-     Octets : 0

OS900#
```

### Continually Updated

To view the *continually updated* (automatically refreshed) statistical information on one or more ports (possibly a port trunk):

1. Enter **enable** mode.
2. Invoke either of the following commands:

   **monitor port statistics PORTS-GROUP [packets]**

   **monitor port statistics table [PORTS-GROUP]**

   where,

   **monitor**: Display with refresh[16]

   **port**: Port related action

   **statistics**: Statistics related action

   **[PORTS-GROUP]**: Group of Ports.
   For a port trunk the format is **tX**, where,
   **X** is a numerical. Example **t3**.
   (If no port number is entered, all ports are displayed.)

   **table**: Tabular format

   **packets**: Packet counters only

[16] Automatic continuous update

Example

```
OS900# monitor port statistics 3

PORTS STATISTICS
================

Port 3      Ethernet counters
---------------------------
Good bytes received                  : 45198670
Good packets received                : 2791284
Good unicast packets received        : 1895642
Good broadcast packets received      : 364301
Good multicast packets received      : 531341
Bytes transmitted                    : 51006743
Packets transmitted                  : 115672
Unicast packets transmitted          : 85475
Broadcast packets transmitted        : 20344
Multicast packets transmitted        : 65131
CRC or Alignment error received      : 0
Undersize received                   : 0
Oversize received                    : 0
Fragments received                   : 0
Jabber received                      : 0
Collisions received and transmitted  : 15

Port 3      RMON Packet Size Distribution Counters
------------------------------------------------
    -   64 Octets : 3012
  65- 127 Octets : 90258
 128- 255 Octets : 248021
 256- 511 Octets : 720915
 512-1023 Octets : 108839
1024-     Octets : 4203
OS900#
```

To exit monitoring (and freeze the display), press Ctrl C or Ctrl Z.

## Clearing

To clear the statistical counters of one or more ports (possibly a port trunk):

1. Enter **enable** mode.
2. Invoke the command:
   **clear ports statistics [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of Ports. For a port trunk the format is **tX**, where, **X** is a numerical. Example **t3**.
   (If no port number is entered, all ports are cleared.)

Example

```
OS900# clear ports statistics 1-4
OS900#
```

# Digital Diagnostics

## SFP Parameters

To view information on the parameters of SFPs in ports (possibly a port trunk), invoke the command:

1. Enter **enable** mode.

2. Invoke the command:
   **`show port sfp-params [PORTS-GROUP]`**

   where,
   **`show`**: Display
   **`port`**: Port related action
   **`sfp-params`**: SFP parameters
   **`[PORTS-GROUP]`**: Group of Ports. For a port trunk the format is **`tX`**, where, **`X`** is a numerical. Example **`t3`**.
   (If no port number is entered, all ports are displayed.)

Example

```
OS900# show port sfp-params 2
SFP ports internal EEPROM data
===============================


SFP EEPROM Diagnostics: (Port 2)
*************************************
Identifier is SFP.
Connector code is LC.
Transceiver subcode is 1000Base-SX.
Serial encoding mechanism is 8B10B.
The nominal bit rate is 2100 Megabits/sec.
Link length using single mode (9 micron) is not supported.
Link length using 50 micron multi-mode fiber is greater than 300m.
Link length using 62.5 micron multi-mode fiber is greater than 150m.
Link length using cooper cable is not supported.
Vendor name is FINISAR CORP.
Vendor PN is FTRJ8519P1BNL
Vendor revision is A
Nominal transmitter output wavelength at room temperature is 850.00 nm.
======================================================================
```

## SFP Diagnostics

To view real-time diagnostic information on SFPs (possibly a port trunk), invoke the command:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show port sfp-diag [PORTS-GROUP]`**

   where,
   **`show`**: Display
   **`port`**: Port related action
   **`sfp-diag`**: SFP diagnostics
   **`[PORTS-GROUP]`**: Group of Ports. For a port trunk the format is **`tX`**, where, **`X`** is a numerical. Example **`t3`**.
   (If no port number is entered, all ports are displayed.)

Example

```
OS900# show port sfp-diag 3

SFP ports internal EEPROM data
==============================
SFP Digital Diagnostics: (Port 3)
*************************************
Description           Real-Time Value
--------------------  ---------------
Temperature (C)/(F):    44/111
Voltage         (V):  3.2998
TX Bias        (mA):  4.836
TX Power (dBm)/(mW):     -5.4/0.290
RX Power (dBm)/(mW):   -23.8/0.004
************************
```

# Virtual Cable Diagnostics (VCD)

## General

Virtual Cable Diagnostics (VCD™) is a tool for testing an electrical data cable connected to a copper port for faults at the OSI Layer 1 and to pinpoint their location. It applies for cables that are longer than 10 meters (33 feet). To perform VCD, only one CLI command needs to be invoked. VCD identifies an electrical data cable fault type as well as its location accurate to 2 m (6.5 ft).

Some of the fault types detectable are:

- Opens
- Shorts
- Bad connectors
- Impedance mismatch
- Polarity mismatch

| | |
|---|---|
| | **Note**<br>To perform VCD, the Spanning-Tree Protocol must first be disabled. |

## Benefits

- Quick & remote analysis of the attached copper cable
- Identification of fault location and type
- Less need for visits by technical support personnel to remote sites
- Reduced network downtime

## Principle of Operation

VCD uses Time-Domain Reflectometry (TDR), a method that works on the same principle as radar. In this method, an energy pulse transmitted through the cable is partially distorted and reflected when it encounters a fault. The VCD mechanism measures the time it takes for the signal to travel down the cable and analyzes its reflected waveform. It then translates this time into distance and the reflected distorted waveform into the associated fault type.

## Procedure

To perform VCD:

1. Enter **enable** mode.
2. Invoke the command:

   **vct [extended] PORTS-GROUP**

where,

**`[extended]`**: Detailed information.

**`PORTS-GROUP`**: Group of Ports.

as shown in the example below.

## Example

Following is a test case example of an 'open' on a 100 meter long cable. One end of the cable was connected to port 2 of the local OS900. The far end of the cable was connected to another switch (in normal operation mode). VCD was performed. The far end of the cable was disconnected and VCD was performed again.

The commands invoked and the test results are shown below.

```
MRV OptiSwitch 910 version d1659-20-06-05
OS900 login: admin
Password:
Last login: Tue Jun 28 07:02:40 2006 on ttyS0
OS900> enable
OS900# vct extended 7
Port 2:
pair#0: No problem found. Cable Length is unknown.
pair#1: No problem found. Cable Length is unknown.
pair#2: No problem found. Cable Length is unknown.
pair#3: No problem found. Cable Length is unknown.
 extended status:
link GE to FE down shift status:  no downshift
OS900# vct extended 7
Port 2:
pair#0: Open in Cable. Approximatly 97 meters from the tested port.
pair#1: Open in Cable. Approximatly 99 meters from the tested port.
pair#2: Open in Cable. Approximatly 100 meters from the tested port.
pair#3: Open in Cable. Approximatly 97 meters from the tested port.
 extended status:
    no extended data for port 2
OS900#
```

# XFP Port Protocol

## General

This section applies to OS900 models with 10 Gbps ports only.

## Setting

To set an OS930 port (10 Gbps XFP) to transmit frames in Ethernet protocol or SONET/SDH protocol format:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port xfp mode lan|wan PORTS-GROUP|all`**

   where,

   **`lan`**: Ethernet format at 10.3 Gbps

   **`wan`**: SONET/SDH format at 9.95328 Gbps (OC-192 or STM-64)

   **`PORTS-GROUP`**: Group of XFP ports.

   **`all`**: All XFP ports.

<u>Example</u>

```
OS930(config)# port xfp mode wan 1
port 13  xfp mode set to: WAN
OS930(config)#
```

## Viewing

### Protocol

To view the protocol in which the XFP ports are set to operate:

1. Enter **enable** mode.
2. Invoke the command:

   **show port details [PORTS-GROUP]**

   where,

   **PORTS-GROUP**: Group of XFP ports.

Example

```
OS930# show port details 1
Port 13 details:
----------------
Description          : N/A
Type                 : ETH10000
Link                 :  ON
Duplex state         : FULL
PHY                  : XFP
XFP mode             : WAN
Speed selected       : FORC10,000
Actual speed         :  10 GBps
Selected cross mode  : AUTO
Bypass mode          : ENABLE
State                : ENABLE
Priority             : 1
Flow control mode    : off
Ethertype            : CORE1:0x8100
OutBound Tagged      : untagged
Tags List            : 100
Udld                 : -
OS930#
```

### WAN Status

To view the *momentary* status of one XFP port that has been set in WAN mode, i.e., set to transmit frames in SONET/SDH format:

1. Enter **enable** mode.
2. Invoke the command:

   **show port xfp wan-status PORT**

   where,

   **PORT**: Number of XFP port.

To view the *continually updated* (automatically refreshed) statistical information on one or more ports:

1. Enter **enable** mode.
2. Invoke the command:

   **monitor port xfp wan-status PORT**

   where,

   **monitor**: Display with refresh

   **PORT**: Number of XFP port.

Example

```
OS930(config)# do show port xfp wan-status 1
Port 1 xfp, wan status:

Section OOF         :  OK
Section LOS         :  OK
Section LOF         :  OK
Section BIP (B1)    :          0
Line AIS            :  OK
Line RDI            :  OK
Line REI            :       9435
Line BIP (B2)       :          0
Path AIS            :  OK
Path REI            :         63
Path BIP (B3)       :          1
Path LOP            :  OK
Path PLM            :  OK
Path RDI            :  OK
Path Remote PLM     :  OK
OS930(config)#
```

## Clearing

To clear the status counters associated with an XFP port set in WAN mode, i.e., set to transmit frames in SONET/SDH format:

1. Enter **enable** mode.
2. Invoke the command:
   **clear port xfp wan-status-counters PORT**
   where,
   **PORT**: Number of XFP port.

# XFP WAN Tx and Rx Trace

## General

This section applies to the OS930 model only.

## Setting

### One Octet at a Time

To set the value of *an* octet in the J1 (path trace) or J0 (section trace) field in the header of SONET/SDH frames transmitted at an OS930 port (10 Gbps XFP) that is in WAN mode:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **port xfp wan-tx-trace (J1|J0) octet <0-15> VALUE (PORTS-GROUP|all)**
   where,
   **J1**: Path Trace.
   **J0**: Section Trace.
   **<0-15>**: Octet number.
   **VALUE**: Octet value (2-digit hexadecimal number).
   **PORTS-GROUP**: Group of XFP ports.
   **all**: All XFP ports.

Example

```
OS930(config)# port xfp wan-tx-trace J1 octet 4 7 1
OS930(config)#
```

### All Octets

To set the value of *all* octets in the J1 (path trace) or J0 (section trace) field in the header of SONET/SDH frames transmitted at an OS930 port (10 Gbps XFP) that is in WAN mode:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port xfp wan-tx-trace (J1|J0) VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE VALUE (PORTS-GROUP|all)`**
   where,
   **`J1`**: Path Trace.
   **`J0`**: Section Trace.
   **`VALUE`**: Octet value (2-digit hexadecimal number).
   **`PORTS-GROUP`**: Group of XFP ports.
   **`all`**: All XFP ports.

Example

In the following example, the first octet in **`J1`** path trace (of the frames to be transmitted) is assigned the value **`3`**, the second **`7`**, the third **`4`**, and so on, for port **`13`**.

```
OS930(config)# port xfp wan-tx-trace J1 3 7 4 8 6 9 1 5 16 14 15 13 2 10 12 11 13
OS930(config)#
```

## Viewing

To view the values that have been set to the octets in the J1 (path trace) or J0 (section trace) field for the header of SONET/SDH frames to be transmitted or received at an OS930 port (10 Gbps XFP):

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show port xfp wan-trace PORTS-GROUP|all`**
   where,
   **`PORTS-GROUP`**: Group of XFP ports.
   **`all`**: All XFP ports.

Example

The following example shows that the first octet in **`J1`** (of the frames to be transmitted) is assigned the value **`3`**, the second **`7`**, the third **`4`**, and so on, for port **`13`**.

```
OS930(config)# do show port xfp wan-trace 13
 P1 J1
  Tx:  03 07 04 08 06 09 01 05 16 14 15 13 02 10 12 11
  Rx:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 P1 J0
  Tx:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 89
  Rx:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00


OS930(config)#
```

# Uni-Directional Link Detection Protocol (UDLD)

## General

UDLD is a Layer 2 protocol that enables a device (e.g., OS900) having Ethernet links to LAN ports via fiberoptic cables to:

– Monitor the physical configuration of the cables
– Detect when Ethernet links are uni-directional
– Disable LAN ports having uni-directional Ethernet links, and

– Generate an alert.

Whereas auto-negotiation (Layer 1 mechanism), for example, handles physical signaling and fault detection, UDLD can detect the identities of neighbor devices and disable misconnected LAN ports.

Thus running auto-negotiation and UDLD concurrently on the OS900 prevents both physical and logical unidirectional connections and consequently malfunctioning of other protocols.

## Applicability

UDLD on the OS900 applies only for 100 and 1000 Mbps fiberoptic Ethernet ports.

## Principle of Operation

A uni-directional link occurs whenever traffic transmitted by the local device over a link is received by the neighbor but traffic transmitted from the neighbor is not received by the local device. This can occur when for instance one of the two fibers in a fiberoptic cable is disconnected.

When UDLD is enabled, the OS900 periodically transmits UDLD packets to neighbor devices on its LAN ports. If the neighbor OS900 or any other device that supports UDLD does not receive UDLD packets for a specific time period, the link is flagged as uni-directional and the LAN port can be disabled.

If conditions on both fibers are OK at Layer 1, UDLD at Layer 2 determines whether the fibers are connected correctly and whether traffic flow is bidirectional between the right neighbors. This determination cannot be made by the auto-negotiation mechanism.

## Requirements

1. For UDLD to be able to identify and break uni-directional links, the devices on both ends of the link are required to support UDLD.
2. For the two SFP ports at the end of the link:
   2.1 Set the type of physical interface to 100Base-X or 1000Base-X using the command:
   **`port media-select sfp|sfp100 PORT-GROUP|all`**
   where,
   **`sfp`**: Set the port to operate as a 1000Base-X interface
   **`sfp100`**: Set the port to operate as a 100Base-X interface
   **`PORT-GROUP`**: Group of Ports
   **`all`**: All ports
   If a 100Base-FX SFP is present, the physical interface is automatically set to 100Base-X, i.e., the argument value **`sfp100`** in the command **`port media-select`** is selected.
   2.2 Set the speed to 100 Mbit/sec or 1000 Mbit/sec using the command:
   **`port speed 100|1000 PORTS-GROUP|all`**
   where,
   **`100`**: 100 Mbit/sec
   **`1000`**: 1000 Mbit/sec
   **`PORTS-GROUP`**: Group of Ports
   **`all`**: All ports

## Configuration

By default UDLD is disabled.

The OS900 can be set in either of the following modes:

– Aggressive Mode
– Non-aggressive Mode (default)

### Aggressive Mode

#### *Enabling*

UDLD Aggressive mode is to be used only on point-to-point links between network devices that support this mode. In this mode, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD attempts to reestablish the connection with the neighbor. Following eight failed attempts, the port is disabled.

The advantage in Aggressive mode becomes evident in the following instances:

- A port on one side of a link neither transmits nor receives, or
- One side of a link is UP while the other is DOWN

In either instance it disables one of the ports on the link thereby preventing packets from being discarded.

To enable UDLD Aggressive mode:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port udld aggressive [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports to be handled in Aggressive UDLD mode.

Example

```
OS910(config)# port udld aggressive 2,4
OS910(config)#port udld enable 4
OS910(config)#
```

#### *Disabling*

To disable UDLD Aggressive mode:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no port udld aggressive [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports to be freed from Aggressive UDLD mode.

Example

```
OS910(config)# no port udld aggressive 4
OS910(config)#
```

### Non-aggressive Mode

#### *Enabling*

UDLD Non-aggressive mode does not disable the port link. With the default interval of 15 seconds it serves satisfactorily in preventing Spanning Tree loops. In this mode, port links are not disabled.

To configure UDLD Non-aggressive mode:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port udld enable [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports to be handled in Non-aggressive UDLD mode.

Example

```
OS910(config)# port udld enable 1,4
OS910(config)#
```

#### *Disabling*

To disable UDLD Non-aggressive mode:

1. Enter **configure terminal** mode.
2. Invoke the command:

**no port udld enable [PORTS-GROUP]**

where,

**[PORTS-GROUP]**: Group of ports to be freed from Non-aggressive UDLD mode.

Example

```
OS910(config)# no port udld enable 1,4
OS910(config)#
```

### VLAN Tag in UDLD Messages

#### *Custom*

If a port (tagged) being handled by UDLD is a member of several VLAN interfaces, by default UDLD messages with the lowest tag of the VLAN interfaces are sent to the device at the other end of the link.

To force inclusion of any (other) VLAN interface tag to be sent with the UDLD messages:

1. Enter **configure terminal** mode.
2. Invoke the command:

**port udld primary-vlan <1-4095> [PORTS-GROUP]**

where,

**<1-4095>**: VLAN tag to be sent with the UDLD messages.

**[PORTS-GROUP]**: Group of ports to send UDLD messages with the selected VLAN tag.

Example

```
OS910(config)# port udld primary-vlan 1000 4
OS910(config)#
```

#### *Default*

To cause messages to be sent in default mode, i.e., with the lowest tag:

1. Enter **configure terminal** mode.
2. Invoke the command:

**no port udld primary-vlan <1-4095> [PORTS-GROUP]**

where,

**<1-4095>**: VLAN tag to be replaced with the lowest tag.

**[PORTS-GROUP]**: Group of ports to send UDLD messages with the lowest VLAN tag.

### UDLD Message Interval

#### *For Uni-directional Ports*

Custom Setting

To set the time interval between UDLD messages on one or more *uni-directional* ports operating in advertisement mode to a new value:

1. Enter **configure terminal** mode.
2. Invoke the command:

**port udld slow-message-interval <7-90> [PORTS-GROUP]**

where,

**<7-90>**: Time interval between UDLD messages in seconds. Default: 7

**[PORTS-GROUP]**: Group of *uni-directional* ports operating in advertisement mode.

Example

```
OS910(config)# port udld slow-message-interval 40 1,4
OS910(config)#
```

Default Setting

To set the time interval between UDLD messages on one or more *uni-directional* ports to the default value (7 seconds):

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no port udld slow-message-interval [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of *uni-directional* ports operating in advertisement mode.

Example

```
OS910(config)# no port udld slow-message-interval 1,4
OS910(config)#
```

***For Bi-directional Ports***

Custom Setting

The default time interval between UDLD messages is 15 seconds.

To set the time interval between UDLD messages on one or more *bi-directional* ports operating in advertisement mode to a new value:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port udld message-interval <7-90> [PORTS-GROUP]**

   where,

   **<7-90>**: Time interval between UDLD messages in seconds.

   **[PORTS-GROUP]**: Group of *uni-directional* ports operating in advertisement mode.

Example

```
OS910(config)# port udld message-interval 35 1,3
OS910(config)#
```

Default Setting

To set the time interval between UDLD messages on one or more *bi-directional* ports to the default value (15 seconds):

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no port udld message-interval [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of *bi-directional* ports operating in advertisement mode.

Example

```
OS910(config)# no port udld message-interval 1,3
OS910(config)#
```

**Reset**

To reset specific ports that have been disabled by UDLD:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port udld reset [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports disabled by UDLD that are to be reset.

## Viewing

### UDLD Status

To view UDLD status on specific ports, invoke the command:

1. Enter **enable** mode.
2. Invoke the command:

   **show port udld [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports whose configuration is to be viewed.

Example

```
OS904# show port udld 4
Port 4
---
Port configuration setting: Enabled
Current link state: UDLD bidirectional link
Current operational state: Advertisement
Message interval: 15
Time out interval: 7
  Entry 1
  ---
  Device ID: 0725000211
  Current neighbor state: Bidirectional
  Device name: OptiSwitch 910
  Port ID: 10
  Neighbor echo:
  Neighbor echo 1 device: 0823001245
  Neighbor echo 1 port: 4
  Message interval: 15
  Timeout interval: 7
  Sequence number: 45
----------------------------------------
OS904#
```

'`Entry 1`' is a list of the data received from the neighbor device.

### Port Status

To view the UDLD status of one or more ports:

1. Enter **enable** mode.
2. Invoke the command:

   **show port details [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports whose configuration is to be viewed.

Example

```
OS904# show port details 4
Port 4 details:
-------------------
Description          : N/A
Type                 : ETH100/1000
Media-select mode    : SFP
Link                 : ON Sfp
Duplex state         : FULL
PHY                  : SFP+100FX
Speed selected       : AUTO
Actual speed         :  1 GBps
Auto-Neg Advertise   : Default
State                : ENABLE
Priority             : 1
Flow control mode    : off
Ethertype            : CORE1:0x8100
OutBound Tagged      : untagged
Tags List            :
Udld                 : Bidirectional link
OS904#
```

## Ingress Counters

An ingress counter is used to count packets in an ingress queue according to one or more of the following attributes:

- Physical ports
- VLAN tag (Interface ID)

There are two sets of four ingress counters, identified as 'set1' and 'set2'. The ingress counters in a set are:

- REC PACKETS (counts the number of received packets)
- DROP VLAN-FILTER (counts the number of packets dropped due to VLAN ID [tag] mismatch, i.e., the VLAN ID of the packets are different from the tag of the ingress VLAN)
- DROP SECURITY (counts the number of packets dropped due to security screening. Security screening includes *Learn Table* limits, e.g., by port or VLAN tag – see *Limiting*, page *112*, – and invalid source address)
- DROP OTHER (counts the number of packets dropped due to drop conditions other than those described for the counters DROP VLAN-FILTER and DROP SECURITY.
  These drop conditions are: Spanning Tree state change and rate limit of flood packets – see ***Chapter 10:*** *Rate Limiting of Flood Packets*, page *249*.)

### Activation

To activate a set of ingress queue counters:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`ingress-counters set1|set2 port PORT|all tag <1-4096>|all`**

   where,

   **`set1`**: First ingress counters set
   **`set2`**: Second ingress counters set
   **`port`**: Ingress port
   **`PORT`**: Range of port numbers from which one is to be selected
   **`all`**: (first) All ports
   **`tag`**: VLAN interface tag

**<1-4096>**: Range of VLAN Interface IDs from which one can be selected. If a value that is the same as the VLAN tag of an existing VLAN is selected, the DROP VLAN-FILTER counter will show zero counts since packets with this VLAN tag (ID) are valid and are therefore *not dropped*!

**all**: (second) All VLAN Interface IDs. (To enable the DROP VLAN-FILTER counter to count all packets who's VLAN IDs are different from the tag of the ingress VLAN, select this option instead of a single tag value in the range **<1-4096>**.)

Example

```
OS900(config)# ingress-counters set2 port 3 tag all
OS900(config)#
```

To revoke the above command, invoke the command:

**no ingress-counters set1|set2**

where,

**set1**: First ingress counters set

**set2**: Second ingress counters set

Example

```
OS900(config)# no ingress-counters set2
OS900(config)#
```

**Viewing**

To view the ingress queue counters

1. Enter **enable** mode.
2. Invoke either of the following commands:

**show ingress-counters set1|set2**

**monitor ingress-counters set1|set2**

where,

**show**: Display *without* refresh.

**monitor**: Display *with* refresh.

**set1**: First ingress counters set

**set2**: Second ingress counters set

Example

```
OS900# show ingress-counters set2
Ingress counters group set2 is active for port 3, tag all

REC        DROP          DROP       DROP
PACKETS    VLAN-FILTER   SECURITY   OTHER
7809153    21            48         67
OS900#
```

**Clearing**

To clear an ingress queue counters

1. Enter **configure terminal** mode.
2. Invoke either of the following commands:

**clear ingress-counters (set1|set2)**

where,

**set1**: First ingress counters set

**set2**: Second ingress counters set

Example

```
OS900(config)# clear ingress-counters set2
OS900(config)#
```

# Chapter 7: Interfaces

## General

This chapter introduces the four types of interface of the OS900. They are:

- Out-of-band RS-232 Interface
- Out-of-band Ethernet Interface
- Dummy Interface
- Inband VLAN interface

Since a considerably wider range of operations can be performed on and with an inband VLAN interface, this chapter is devoted almost exclusively to this type of interface.

## Purpose

Interfaces are needed for VLANs, Access Lists, management, and protocols of various OSI layers, such as, Layer 2.

## Out-of-band RS-232 Interface

The out-of-band RS-232 interface (***CONSOLE EIA-232*** Port – see Front Panel of OS900) is used for *local* management only and is described in the section *CONSOLE EIA-232*, page *66*. The connection of a craft terminal to the RS-232 interface is described in the section *Craft Terminal/Emulator (For Out-of-band Management)*, page *81*. The required setup of the craft terminal is described in the section *Local Management (Craft Terminal)*, page *83*.

## Out-of-band Ethernet Interface

### General

The out-of-band Ethernet interface (***MGT ETH*** Port – see Front Panel of OS900) is used for *remote* management only and is described in the section *MGT ETH*, page *66*. The connection of a management station is described in the section *TELNET/SSH Station or SNMP NMS*, page *81*. Unlike the RS-232 interface, management via the out-of-band Ethernet interface is, by default, disabled for security reasons. The procedure for enabling management via the out-of-band Ethernet interface is given in the section *Remote Management*, just below.

### Remote Management

#### Enabling

To *enable* remote management (SNMP, TELNET, SSH, or TFTP) via the out-of-band Ethernet interface:

1. Enter **`configure terminal`** mode.

   Example

   ```
   OS900# configure terminal
   OS900(config)#
   ```

2. Enter the out-of-band Ethernet interface (***MGT ETH*** Port on Front Panel of OS900) mode by invoking the command:

   **`interface out-of-band eth0`**

Example

```
OS900(config)# interface out-of-band eth0
OS900(config-eth0)#
```

3. Assign an IP address to the out-of-band interface by invoking the command:

   **`ip A.B.C.D/M`**

   where,

   **`A.B.C.D/M`**: IP address/Mask of the interface. The mask can be up to 31 bits long.

Example

```
OS900(config-eth0)# ip 193.07.222.11/24
OS900(config-eth0)#
```

4. Enable management by invoking the command:

   **`management [snmp|telnet|ssh|tftp] [SOURCE_IPV4_ADDRESS]`**

   where,

   **`snmp`**: Enable SNMP management

   **`telnet`**: Enable TELNET management

   **`ssh`**: Enable SSH management

   **`tftp`**: Enable TFTP server on the OS900 and allow TFTP clients to access configuration files stored in the OS900

   **`[SOURCE_IPV4_ADDRESS]`**: IP address of the management host or management subnet (IP address/mask). The mask can be up to 31 bits long.

Example

```
OS900(config-eth0)# management snmp 192.2.2.2/24
OS900(config-eth0)#
```

**Notes**

1. More than one of the management protocols (SNMP, SSH, TELNET, and TFTP) may be selected with which the OS900 will be accessible by repeating the command:

   **`management snmp|telnet|ssh|tftp [SOURCE_IPV4_ADDRESS]`**

2. The command:

   **`management snmp|telnet|ssh|tftp`**

   (i.e., without the IP address)

   enables management from any IP host with the specified protocol.

3. The command:

   **`management`**

   (i.e., without the protocol and without the IP address)

   enables SNMP, TELNET, and SSH management from any IP host.

   (TFTP is not enabled with this command for security reasons. To enable TFTP, the command **`management tftp`** must be invoked.)

4. Up to 20 instances (protocols together with IP addresses) can be configured per VLAN interface.

### Disabling

To *disable* remote management (SNMP, TELNET, SSH, or TFTP) via the out-of-band Ethernet interface:

1. Enter **`configure terminal`** mode.

Example

```
OS900# configure terminal
OS900(config)#
```

2. Enter the out-of-band Ethernet interface mode by invoking the command:

**interface out-of-band eth0**

Example

```
OS900(config)# interface out-of-band eth0
OS900(config-eth0)#
```

3. Disable management by invoking the command:
   **no management [snmp|telnet|ssh|tftp] [SOURCE_IPV4_ADDRESS]**
   where,
   **snmp**: Disable SNMP management
   **telnet**: Disable TELNET management
   **ssh**: Disable SSH management
   **tftp**: Disable TFTP server on the OS900
   **[SOURCE_IPV4_ADDRESS]**: IP address of the management host.

Example

```
OS900(config-eth0)# no management snmp 192.2.2.2/24
OS900(config-eth0)#
```

**Note**

The command:

**no management**

(i.e., without the protocol and without the IP address)

disables SNMP, TELNET, SSH, as well as TFTP management from any IP host.

## TFTP Server Mode

### General

The OS900 operates as a TFTP server.

A TFTP client can be connected to an OS900 interface in order to back up the configuration files stored in the OS900.

Another way to back up IP configuration files is to first set the OS900 as an FTP client and then to invoke the command:

**copy ftp startup-config FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]**

as described in the section *Download*, page *523*.

### Enabling

To *enable* access via the out-of-band Ethernet interface for a TFTP client:

1. Enter **configure terminal** mode.

Example

```
OS900# configure terminal
OS900(config)#
```

2. Select the out-of-band Ethernet interface via which access is to be enabled for a TFTP client by invoking the command:
   **interface out-of-band eth0**

Example

```
OS900(config)# interface out-of-band eth0
OS900(config-eth0)#
```

3. Enable access for a TFTP client by invoking the command:
   **management tftp [SOURCE_IPV4_ADDRESS]**
   where,

**tftp**: Enable TFTP server on the OS900 and allow TFTP clients to access configuration files stored in the OS900

**[SOURCE_IPV4_ADDRESS]**: IP address (with or without mask) of the TFTP client. The mask can be up to 31 bits long.

Example

```
OS900(config-eth0)# management tftp 193.222.48.105/24
OS900(config-eth0)#
```

**Disabling**

To *disable* access via the out-of-band Ethernet interface for a TFTP client:

1. Enter **configure terminal** mode.
2. Select the out-of-band Ethernet interface via which access is to be disabled for a TFTP client by invoking one of the following commands:
   **interface out-of-band eth0**

   Example

   ```
   OS900(config)# interface out-of-band eth0
   OS900(config-eth0)#
   ```
3. Disable access for a TFTP client by invoking the command:
   **no management tftp [SOURCE_IPV4_ADDRESS]**
   where,
   **tftp**: Disable TFTP server on the OS900
   **[SOURCE_IPV4_ADDRESS]**: IP address (with or without mask) of the TFTP client. The mask can be up to 31 bits long.

   Example

   ```
   OS900(config-eth0)# no management tftp 193.222.48.105/24
   OS900(config-eth0)#
   ```

## Deleting

To delete the existing out-of-band Ethernet interface:

1. Enter **configure terminal** mode.

   Example

   ```
   OS900# configure terminal
   OS900(config)#
   ```
2. Delete the existing out-of-band Ethernet interface by invoking the command:
   **no interface out-of-band eth0**

   Example

   ```
   OS900(config)# no interface out-of-band eth0
   OS900(config-eth0)#
   ```

# Dummy Interface

## General

A dummy interface is a software-only loopback interface. It emulates an interface that is always up and has connectivity to all VLAN interfaces of the OS900.

Up to 100 dummy interfaces can be configured.

## Configuration

To configure a dummy interface:

1. Enter **configure terminal** mode.
2. Invoke the command:

**interface dummy IFNAME**

where,

**IFNAME**: ID of interface. (The ID must have the format **dummyX**, where **X** can be any integer in the range **1-100**, e.g., dummy30.)

Example

```
OS900(config)# interface dummy dummy3000
OS900(config-dummy3000)#
```

# Inband VLAN interfaces

## General

Inband VLAN interfaces are user-creatable VLANs, each of which can be assigned an IP address. A VLAN is a logical grouping of one or more ports to form an isolated communication domain. Communication between ports of the same VLAN occurs as if the ports are connected to the same physical LAN. VLAN interfaces are used for data communication but can concurrently be used also for inband management. The management station can be connected to any of the data ports (indicated in *Figure 2*, page *65*). Unlike the RS-232 interface, management via a VLAN interface is, by default, disabled for security reasons. The procedure for enabling management via *a* VLAN interface is given in the section *Remote Management*, page *191*.

## Number

The maximum number of VLAN interfaces that can be configured is 4K.

## IDs

When configuring a VLAN interface, an Interface ID must be assigned to it using the format **vifX**, where **X** is a decimal number in the range **1-4095**. Examples of Interface IDs are: **vif1**, **vif2**, **vif3**, … **vif4095**. **vif0** is reserved for the Default Forwarding VLAN interface – described in the section *Default Forwarding VLAN Interface*, page *185*.

## Configuring

To configure a VLAN interface:

1. Enter **configure terminal** mode.

   Example

   ```
   OS900# configure terminal
   OS900(config)#
   ```

2. Assign an Interface ID to the VLAN interface by invoking the command:

   **interface vlan IFNAME**

   where,

   **vlan**: VLAN

   **IFNAME**: Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095

   Example

   ```
   OS900(config)# interface vlan vif2005
   OS900(config-vif2005)#
   ```

3. Assign ports to the VLAN interface by invoking the command:

   **ports PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports to be members of the VLAN interface.

   Example

   ```
   OS900(config-vif2005)# ports 2-4
   ```

```
OS900(config-vif2005)#
```

4. Define a tag (VID) for the VLAN interface by invoking the command:

   **`tag TAG`**

   where,

   **`TAG`**: User-selectable tag (VID) for the VLAN interface. The tag can have any value in the range 1-4095.

Example

```
OS900(config-vif2005)# tag 3000
Interface is activated.
```

| Note |
|---|
| When valid ports and a tag are assigned to an interface, the VLAN interface becomes active as shown in the example above. |

A VLAN interface can be in either one of the following three *states*:

**`NA`**: Not Active, possibly because port *or* tag is not assigned to the VLAN interface

**`UP`**: Active and link exists on one or more ports that are members of the VLAN interface

**`DO`**: Active and no link on any of the ports that are members of the VLAN interface

5. (Optional) For inband management, assign an IP address to the VLAN interface by invoking the command:

   **`ip A.B.C.D/M`**

   where,

   **`A.B.C.D/M`**: IP address/Mask of the VLAN interface.
   The mask can be up to 31 bits long.
   Valid values are up to 223.255.255.254.
   223.255.255.255 is the broadcast value.
   224.0.0.0 to 239.255.255.255 is the multicast range.

Up to 15 IP addresses can be assigned to a VLAN interface by repeatedly invoking the above command **`ip A.B.C.D/M`**.

To delete an IP address, invoke the command:

**`no ip A.B.C.D/M`**

where,

**`A.B.C.D/M`**: IP address/Mask of the VLAN interface.
The mask can be up to 31 bits long.
Valid values are up to 223.255.255.254.
223.255.255.255 is the broadcast value.
224.0.0.0 to 239.255.255.255 is the multicast range.

Example

```
OS900(config-vif2005)# ip 193.86.205.47/24
OS900(config-vif2005)#
```

6. (Optional) Set the modes of the ports (that are to be included in the interface) as described in the section *Outbound Tag Mode*, page *137*.

   To include a port in two or more VLAN interfaces, one of the following must be done:

   – The port must first be set as **`tag`** or **`hybrid`** type in outbound tag mode (as described in the section *Outbound Tag Mode*, page *137*).

   – The port must be set as **`untagged`** in outbound tag mode (as described in the section *Outbound Tag Mode*, page *137*) and enabled for multi-VLAN membership (as described in the section *Multi-VLAN Membership for Untagged Ports*, page *139*). This is so because it is not possible to create overlapping VLANs with untagged ports since an untagged port can be a member of only one VLAN interface.

Example

```
OS900(config)# port tag-outbound-mode tagged 1,4
OS900(config)#
```

7. (Optional) Set the bandwidth limit for Layer 3 protocols by invoking the command:
   **bandwidth BANDWIDTH**
   where,
   **BANDWIDTH**: Bandwidth in the range <**1-10000000000** bits> (valid units are: **k** (kilo), **m** (Mega), **g**(Giga). Example: **200m**.

Example

```
OS910(config-vif249)# bandwidth 10g
OS910(config-vif249)#
```

8. (Optional) Increase the size of packets to be forwarded to the CPU to the MTU by invoking the command:
   **mtu MTU**
   where,
   **MTU**: MTU size.

| | **Note** |
|---|---|
| | If different MTUs are defined for a VLAN interface (as described in the section *Setting for Ports*, page *115*), member ports (as described in the section *Setting for VLAN Interfaces*, page *115*), and CPU (as described in the section *Configuring*, page *181*, Step *8*) the smallest of the MTUs will be selected by the OS900. |

9. (Optional) This command is to be invoked when double-tagged packets, namely, packets with a provider tag and a customer tag, are present in management traffic and are to be transmitted toward the customer VLAN via the inband VLAN interface of the intervening OS900.
   To enable transmission of such double-tagged packets via the intervening OS900, invoke the command:
   **management c-tag <1-4095> [c-vpt <0-7>]**
   where,
   **<1-4095>**: Tag of the packets to be received at the customer VLAN.
   **<0-7>**: VPT value of customer tag.
   (To prevent transmission of such double-tagged packets via the inband VLAN interface, invoke the command: **no management c-tag <1-4095> [c-vpt <0-7>]**.)

Example

```
OS910(config-vif249)# management c-tag 27 c-vpt 4
OS910(config-vif249)#
```

## Name

The default name of a VLAN interface is the same as its Interface ID. This name (or any other) can be changed (for example, to one that serves as a mnemonic for conveniently identifying the interface).

To change the name of an interface:

1. Enter the **configure terminal** mode.
2. Access the mode of an existing VLAN interface by invoking the command:
   **interface IFNAME**
   where,
   **IFNAME**: Interface ID of an existing interface (e.g., **vif1**, **vif2**, etc.)

3. Change the name of the VLAN interface by invoking the command:
   **name NAME**
   where,
   **name**: Name.
   **NAME**: Name for VLAN interface.

Example

```
OS900# configure terminal
OS900(config)# interface vif7
OS900(config-vif7)# show

Name     M Device        IP                  State MAC                Tag  Ports
-------------------------------------------------------------------------------
vif7       vif7          192.2.2.2/24         DO    00:0F:BD:00:05:B8  0010 1-3

OS900(config-vif7)# name Tiger
OS900(config-vif7)# show

Name     M Device        IP                  State MAC                Tag  Ports
-------------------------------------------------------------------------------
Tiger      vif7          192.2.2.2/24         DO    00:0F:BD:00:05:B8  0010 1-3

OS900(config-vif7)#
```

## Description

To enter a textual description of an interface:

1. Enter **configure terminal** mode.
2. Access the mode of an existing VLAN interface by invoking the command:
   **interface IFNAME**
   where,
   **IFNAME**: Interface ID of an existing interface (e.g., **vif1**, **vif2**, etc.)
3. Enter a textual description of the interface by invoking the command:
   **description ..**
   where,
   **description**: Textual description.
   **..**: Textual description.

Example

```
OS900(config-vif2005)# description This interface is for Customer 10
OS900(config-vif2005)# show detail

vif2005 is DOWN (No state changes have occurred)
  Description: This interface is for Customer 10
  Active: Yes
  Ports: 6-8,10
  Interface type is Vlan
  Encapsulation: 802.1Q,  Tag 3000
  MAC address is 00:0F:BD:02:05:B8
  IP address is 193.86.205.47/24
  Cpu-membership is enable
  Management access is denied
  TFTP access is denied.
  Access-group is not defined

OS900(config-vif2005)#
```

## Default Forwarding VLAN Interface

### General

The Default Forwarding VLAN interface is a broadcast domain for all ports not included in user-defined VLAN interfaces. That is, any packet entering one such port is flooded to all other such ports.

In the factory default setting, only the default VLAN interface (**vif0**) exists and all the physical data ports of the OS900 are untagged members of it. The default VLAN interface cannot be deleted. However, any of its (member) ports can be assigned to a user-defined VLAN interface (thereby removing the port from 'Default Forwarding VLAN interface'). The default tag (VLAN ID) for **vif0** is **1**.

### Viewing

To view the default forwarding status and the default tag:

1. Enter **enable** mode.
2. Invoke the command:
   **show default-fwd**

Example

```
OS900> enable
OS900# show default-fwd
default forwarding tag : 1
OS900#
```

### Tag Modification

The default tag (or any other tag assigned to **vif0**) can be changed as follows:

1. Enter **configure terminal** mode.
2. Change the tag of the Default Forwarding VLAN interface by invoking the command:
   **default-fwd tag TAG**
   where,
   **TAG**: VLAN ID. It can be any number in the range 1-4095.

Below is an example showing:

– Display of the tag of **vif0** using the command **show interface**. The tag ID is shown in the `Tag` column. In the example, the tag ID is `0001`.

– Change of the default tag to 2007 using the command default-fwd tag 2007.

– Display of the new tag of **vif0** using the command **show interface**. The system shows that it is `2007`.

```
OS900(config)# show interface

INTERFACES TABLE
================
Name     M Device       IP                State MAC               Tag  Ports
-------------------------------------------------------------------------------
vif0       vif0         -                  DO   00:0F:BD:00:05:B8 0001 1-10

- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

OS900(config)# default-fwd tag 2007
OS900(config)# show interface

INTERFACES TABLE
================
Name     M Device       IP                State MAC               Tag  Ports
-------------------------------------------------------------------------------
vif0       vif0         -                  DO   00:0F:BD:00:05:B8 2007 1-10
```

```
- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

OS900(config)#
```

### Disabling

The Default Forwarding VLAN Interface is by default *enabled*. To disable it:

1. Enter **`configure terminal`** mode.
2. Disable the Default Forwarding VLAN Interface by invoking the command:
   **`no default-fwd`**

Below is an example showing:

- That the Default Forwarding VLAN Interface is initially enabled (by default) as indicated by the response '`default forwarding tag : 1`' to the command **`do show default-fwd`**. (The prefix **`do`** is used with **`show default-fwd`** because the command **`show default-fwd`**, which belongs in the **`enable`** mode, is invoked in another mode, namely, **`configure terminal`** mode.)
- Disabling the Default Forwarding VLAN Interface by invoking the command **`no default-fwd`**.
- Verifying that the Default Forwarding VLAN Interface is disabled as indicated by the response '`default forwarding is disabled`' to the command **`do show default-fwd`**.

```
OS900(config)# do show default-fwd
default forwarding tag : 1
OS900(config)# no default-fwd
OS900(config)# do show default-fwd
default forwarding is disabled
OS900(config)#
```

### Enabling

The Default Forwarding VLAN Interface is by default *enabled*. To enable it:

1. Enter **`configure terminal`** mode.
2. Enable the Default Forwarding VLAN Interface by invoking the command:
   **`default-fwd tag TAG`**
   where,
   **`TAG`**: VID. It can be any number in the range 1-4095.

Below is an example showing:

- That the Default Forwarding VLAN Interface is initially disabled as indicated by the response '`default forwarding is disabled`' to the command **`do show default-fwd`**. (The prefix **`do`** is used with **`show default-fwd`** because the command **`show default-fwd`**, which belongs in the **`enable`** mode, is invoked in another mode, namely, **`configure terminal`** mode.)
- Enabling the Default Forwarding VLAN Interface by invoking the command **`default-fwd tag 1`**.
- Verifying that the Default Forwarding VLAN Interface is enabled as indicated by the response '`default forwarding tag : 1`' to the command **`do show default-fwd`**.

```
OS900(config)# do show default-fwd
default forwarding is disabled
OS900(config)# default-fwd tag 1
OS900(config)# do show default-fwd
default forwarding tag : 1
OS900(config)#
```

## Drop Tag

Drop Tag is a VLAN interface tag for internal use of the OS900. It cannot be assigned to another VLAN interface. However, it can be changed. Its default value is 4094.

### Viewing

To view the (current) Drop Tag:

1. Enter **enable** mode
2. Display the drop tag by invoking the command:
   **show interface**

Below is an example showing the (current) Drop Tag.

```
OS900# show interface

INTERFACES TABLE
================
Name     M Device       IP                State MAC               Tag  Ports
--------------------------------------------------------------------------------
Tiger      vif7         192.2.2.2/24       DO   00:0F:BD:00:05:B8 0010 1-3
vif0       vif0         -                  DO   00:0F:BD:00:05:B8 0001 4-10

- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

OS900#
```

### Changing

To change the (current) Drop Tag:

1. Enter **configure terminal** mode
2. Change the value of the Drop Tag VLAN interface by invoking the command:
   **drop-tag TAG**
   where,
   **TAG**: VID. It can be any number in the range 2-4095. The number '1' is, by default, the tag of the Default Forwarding VLAN interface **vif0**.

   To change the value of the Drop Tag VLAN interface to the default value, i.e., 4094, invoke either of the following commands:
   **no drop-tag**
   **default drop-tag**

Below is an example showing how to change the current Drop Tag (displayed in the above example as 4094) and the changed Drop Tag (38).

```
OS900(config)# drop-tag 38
OS900(config)# show interface

INTERFACES TABLE
================
Name     M Device       IP                State MAC               Tag  Ports
--------------------------------------------------------------------------------
Tiger      vif7         192.2.2.2/24       DO   00:0F:BD:00:05:B8 0010 1-3
vif0       vif0         -                  DO   00:0F:BD:00:05:B8 0001 4-10

- 'vif0' is the default forwarding interface.
-  drop-tag is 38.

OS900(config)#
```

## Drop Packets

To cause the OS900 to drop any one or more ingress packet types at a VLAN:

1. Enter the mode of the interface at which one or more ingress packet types are to be dropped by invoking the command:
   **`interface vlan IFNAME`**
   where,
   **`IFNAME`**: Interface ID having the format **`vifX`**, where **`X`** is a decimal number in the range **`1-4095`**.
2. Invoke the command:
   **`drop ipv4-broadcast|ipv4-multicast|ipv6-multicast|non-ip-broadcast|non-ip-multicast|unknown-unicast`**
   where,
   **`drop`**: Drop packets
   **`ipv4-broadcast`**: Drop IPv4 broadcast packets
   **`ipv4-multicast`**: Drop IPv4 multicast packets (Mac DA = `01:00:5E:XX:XX:XX`)
   **`ipv6-multicast`**: Drop ipv6 multicast packets (Mac DA = `33:33:XX:XX:XX:XX`)
   **`non-ip-broadcast`**: Drop non-IP broadcast packets
   **`non-ip-multicast`**: Drop non-IP multicast packets
   **`unknown-unicast`**: Drop unknown unicast packets

<u>Example</u>

```
OS900(config)# interface vlan vif7
OS900(config-vif7)# ports 3,4
OS900(config-vif7)# tag 100
Interface is activated.

OS900(config-vif7)# drop ipv6-multicast
OS900(config-vif7)#
```

## Viewing

To view an existing interface:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show interface [INTERFACE|configuration|detail|statistics]`**
   where,
   **`INTERFACE`**: Interface ID of an existing interface (e.g., **`vif1`**, **`vif2`**, etc.)
   **`configuration`**: Run-time configuration of interface
   **`detail`**: Details on interface
   **`statistics`**: Statistics on interface

Below is an example showing display of a specific interface.

```
OS900# show interface vif2005

Name    M Device       IP                State MAC               Tag  Ports
----------------------------------------------------------------------------
vif2005   vif2005      193.86.205.47/24   DO   00:0F:BD:02:05:B8 3000 3-5
OS900#
```

Below is an example showing display of details on a specific interface.

```
OS900# show interface detail vif2

vif2 is DOWN (No state changes have occurred)
  Active: Yes
  Ports: 1-4
  Interface type is Vlan
```

```
  Encapsulation: 802.1Q,  Tag 10
  MAC address is 00:0F:BD:00:6E:54
  IP address is 192.83.1.1/24
  Cpu-membership is enable
  Management access is denied
  TFTP access is denied.
  IP forwarding is enabled
  MTU Profile: 1
  MTU:         1500
  Lt learning is enabled
  Access-group is not defined

NSM info:
  index 6, metric 1, mtu 1500 <BROADCAST,MULTICAST>
  HWaddr: 00:0f:bd:00:6e:54
  Bandwidth 10m
  inet 192.83.1.1/24 broadcast 192.83.1.255
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

OS900#
```

Below is an example showing display of statistics of a port that is a member of a specific interface. The display applies to packets received or sent by the CPU.

```
OS900# show interface statistics vif7

The following counters count only frames received and transmitted by the CPU !!!

%Note: vif7 is DOWN

vif7      Link encap:Ethernet  HWaddr 00:0F:BD:00:5E:A0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:59
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:17
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

OS900#
```

## Modifying

To modify any one or more characteristics (e.g., port membership, tag, IP address, etc.) of an existing VLAN interface:

1. Enter **`configure terminal`** mode.
2. Access the mode of the VLAN interface by invoking the command:
   **`interface IFNAME`**
   where,
   **`IFNAME`**: Interface ID of an existing interface (e.g., **`vif1`**, **`vif2`**, etc.)
3. Set the new characteristic(s).

Below is an example showing the current member ports of a specific interface, e.g., `vif7`, how ports can be added and deleted, and the final member ports of the interface.

```
OS900(config-vif7)# show

Name    M Device       IP                State MAC              Tag  Ports
-------------------------------------------------------------------------------
Tiger     vif7         192.88.22.234/24   DO   00:0F:BD:15:05:B8 0100 1
```

```
OS900(config-vif7)# ports add 2-4
OS900(config-vif7)# ports del 1
OS900(config-vif7)# show

Name    M Device       IP                 State MAC               Tag  Ports
------------------------------------------------------------------------------
Tiger     vif7         192.88.22.234/24    DO   00:0F:BD:15:05:B8 0100 2-4

OS900(config-vif7)#
```

## Enabling

A VLAN interface is enabled by default when member ports and a tag are defined for the interface.
To enable an existing VLAN interface:

1. Enter **configure terminal** mode.
2. Enter the mode of the VLAN interface that is to be enabled by invoking the command:
   **interface IFNAME**
   where,
   **IFNAME**: Interface ID of an existing interface (e.g., **vif1**, **vif2**, etc.)
3. *Enable* the VLAN interface by invoking the command **enable**.

Example

```
OS900# configure terminal
OS900(config)# interface vif2005
OS900(config-vif2005)# enable
OS900(config-vif2005)#
```

4. Verify that the VLAN interface is active in the **interface** mode by invoking the command **show detail**.

Example

```
OS900(config-vif7)# show detail

vif7 is DOWN (No state changes have occurred)
  Name: Tiger
  Active: Yes
  Ports: 1-3
  Interface type is Vlan
  Encapsulation: 802.1Q,  Tag 10
  MAC address is 00:0F:BD:00:05:B8
  IP address is 192.2.2.2/24
  Cpu-membership is enable
  Management access is denied
  TFTP access is denied.
  Access-group is not defined
OS900(config-vif7)#
```

## Disabling

An existing VLAN interface can be disabled for administrative reasons or in order to be able to modify several of its characteristics together. To disable an existing VLAN interface:

1. Enter **configure terminal** mode.
2. Enter the mode of the VLAN interface that is to be disabled by invoking the command:
   **interface IFNAME**
   where,
   **IFNAME**: Interface ID of an existing interface (e.g., **vif1**, **vif2**, etc.)
3. *Disable* the VLAN interface by invoking the command **no enable**.

Example

```
OS900# configure terminal
OS900(config)# interface vif2005
OS900(config-vif2005)# no enable
OS900(config-vif2005)#
```

## Remote Management

### Enabling

To *enable* remote management (using any of the protocols SNMP, TELNET, SSH, or TFTP) via a specific VLAN interface:

1. Enter **configure terminal** mode.

   Example

   ```
   OS900# configure terminal
   OS900(config)#
   ```

2. Select the existing VLAN interface via which management is to be enabled by invoking the command:

   **interface IFNAME**

   where,

   **IFNAME**: ID of an existing VLAN interface (e.g., **vif1**, **vif2**, etc.).

   Example

   ```
   OS900(config)# interface vif2
   OS900(config-vif2)#
   ```

3. Enable management by invoking the command:

   **management [snmp|telnet|ssh|tftp] [SOURCE_IPV4_ADDRESS]**

   where,

   **snmp**: Enable SNMP management

   **telnet**: Enable TELNET management

   **ssh**: Enable SSH management

   **tftp**: Enable TFTP server on the OS900 and allow TFTP clients to access configuration files stored in the OS900

   **[SOURCE_IPV4_ADDRESS]**: IP address of the management host or management subnet (IP address/mask). The mask can be up to 31 bits long.

   Example

   ```
   OS900# configure terminal
   OS900(config)# interface vif2
   OS900(config-vif2)# management snmp 193.222.48.105/24
   OS900(config-vif2)#
   ```

**Notes**

1. More than one of the management protocols (SNMP, SSH, TELNET, and TFTP) may be selected with which the OS900 will be accessible by repeating the command:

   **management snmp|telnet|ssh|tftp [SOURCE_IPV4_ADDRESS]**

2. The command:

   **management snmp|telnet|ssh|tftp**

   (i.e., without the IP address)

   enables management from any IP host with the specified protocol.

3. The command:

   **management**

   (i.e., without the protocol and without the IP address)

| | |
|---|---|
| | enables SNMP, TELNET, and SSH management from any IP host. (TFTP is not enabled with this command for security reasons. To enable TFTP, the command **`management tftp`** must be invoked.)<br>4. Up to 20 instances (protocols together with IP addresses) can be configured per VLAN interface. |

### Disabling

To *disable* remote management (using any of the protocols SNMP, TELNET, SSH, or TFTP) via a specific VLAN interface:

1. Enter **`configure terminal`** mode.

   Example

   ```
   OS900# configure terminal
   OS900(config)#
   ```

2. Select the existing VLAN interface via which management is to be disabled by invoking the command:

   **`interface IFNAME`**

   where,

   **`IFNAME`**: ID of an existing VLAN interface (e.g., **`vif1`**, **`vif2`**, etc.).

   Example

   ```
   OS900(config)# interface vif2
   OS900(config-vif2)#
   ```

3. Disable management by invoking the command:

   **`no management [snmp|telnet|ssh|tftp] [SOURCE_IPV4_ADDRESS]`**

   where,

   **`snmp`**: Disable SNMP management

   **`telnet`**: Disable TELNET management

   **`ssh`**: Disable SSH management

   **`tftp`**: Disable TFTP server on the OS900

   **`[SOURCE_IPV4_ADDRESS]`**: IP address of the management host.

   Example

   ```
   OS900# configure terminal
   OS900(config)# interface vif2
   OS900(config-vif2)# no management snmp 193.222.48.105/24
   OS900(config-vif2)#
   ```

**Note**

The command:

**`no management`**

(i.e., without the protocol and without the IP address)

disables SNMP, TELNET, SSH, as well as TFTP management from any IP host.

## TFTP Server Mode

### General

The OS900 operates as a TFTP server.

A TFTP client can be connected to an OS900 interface in order to back up the configuration files stored in the OS900.

Another way to back up IP configuration files is to first set the OS900 as an FTP client and then to invoke the command:

**`copy ftp startup-config FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]`**

as described in the section *Download*, page *523*.

### Enabling

To *enable* access via a specific VLAN interface for a TFTP client:

1. Enter **`configure terminal`** mode.

   Example
   ```
   OS900# configure terminal
   OS900(config)#
   ```

2. Select the existing VLAN interface via which access is to be enabled for a TFTP client by invoking the command:

   **`interface IFNAME`**

   where,

   **`IFNAME`**: ID of an existing VLAN interface (e.g., **`vif1`**, **`vif2`**, etc.).

   Example
   ```
   OS900(config)# interface vif2
   OS900(config-vif2)#
   ```

3. Enable access for a TFTP client by invoking the command:

   **`management tftp [SOURCE_IPV4_ADDRESS]`**

   where,

   **`tftp`**: Enable TFTP server on the OS900 and allow TFTP clients to access configuration files stored in the OS900

   **`[SOURCE_IPV4_ADDRESS]`**: IP address (with or without mask) of the TFTP client. The mask can be up to 31 bits long.

   Example
   ```
   OS900# configure terminal
   OS900(config)# interface vif2
   OS900(config-vif2)# management tftp 193.222.48.105/24
   OS900(config-vif2)#
   ```

### Disabling

To *disable* access via a specific VLAN interface for a TFTP client:

1. Enter **`configure terminal`** mode.
2. Select the existing VLAN interface via which access is to be disabled for a TFTP client by invoking the command:

   **`interface IFNAME`**

   where,

   **`IFNAME`**: ID of an existing VLAN interface (e.g., **`vif1`**, **`vif2`**, etc.).

   Example
   ```
   OS900(config)# interface vif2
   OS900(config-vif2)#
   ```

3. Disable access for a TFTP client by invoking the command:

   **`no management tftp [SOURCE_IPV4_ADDRESS]`**

   where,

   **`tftp`**: Disable TFTP server on the OS900

   **`[SOURCE_IPV4_ADDRESS]`**: IP address (with or without mask) of the TFTP client. The mask can be up to 31 bits long.

   Example
   ```
   OS900# configure terminal
   OS900(config)# interface vif2
   OS900(config-vif2)# no management tftp 193.222.48.105/24
   OS900(config-vif2)#
   ```

## Statistics

Statistical information on an interface involves only traffic going from and to the OS900's CPU via the interface.

### Momentary

To view the *momentary* statistical information on one or more interfaces:

1. Enter **enable** mode or **configure terminal** mode.
2. Invoke the command:

   **show interface statistics [IFNAME]**

   where,

   **show**: Display momentary

   **interface**: Interface-related action

   **statistics**: Statistics-related action

   **[IFNAME]**: Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095. If this argument is omitted, statistics for all interfaces are displayed.

Example

```
OS900# show interface statistics vif7

The following counters count only frames received and transmitted by the CPU !!!

vif7      Link encap:Ethernet  HWaddr 00:0F:BD:00:05:B8
          inet addr:192.28.173.56  Bcast:192.83.173.255  Mask:255.255.255.0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:348209 errors:0 dropped:0 overruns:0 frame:0
          TX packets: 348209 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:72045813 (0.0 B)  TX bytes: 72045813 (0.0 B)
OS900#
```

(Alternatively, momentary statistical information on a specific interface can be viewed by entering the mode of the interface[17] and invoking the command **show statistics**.)

### Continually Updated

To view the *continually updated* (automatically refreshed) statistical information on one or more interfaces:

1. Enter **enable** mode.
2. Invoke the command:

   **monitor interface statistics [IFNAME]**

   where,

   **monitor**: Display with refresh

   **interface**: Interface-related action

   **statistics**: Statistics-related action

   **[IFNAME]**: Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095. If this argument is omitted, statistics for all interfaces are displayed.

To exit monitoring, press Ctrl C or Ctrl Z.

(Alternatively, continually updated statistical information on a specific interface can be viewed by entering the mode of the interface and invoking the command **monitor statistics**.)

[17] To enter the mode of an interface, entering **configure terminal** mode and then invoking the command **interface vlan IFNAME**)

### Deleting

To delete an existing VLAN interface:

1. Enter **`configure terminal`**

   Example
   ```
   OS900# configure terminal
   OS900(config)#
   ```
2. Delete the existing VLAN interface by invoking the command:

   **`no interface IFNAME`**

   where,

   **`IFNAME`**: ID of the existing interface (e.g., **`vif1`**, **`vif2`**, etc.).

   Example
   ```
   OS900(config)# no interface vif1
   interface vif1 was deleted
   OS900(config)#
   ```

## Bridging an Inband VLAN Interface to the Out-of-band Ethernet Interface

### General

One or more Inband VLAN Interfaces can be bridged to the Out-of-band Ethernet Interface (***MGT ETH*** Port – see Front Panel of OS900). Each Inband VLAN Interface that is bridged to the Out-of-band Ethernet Interface will have access to the traffic at the Out-of-band Ethernet Interface. However, all other traffic at one Inband VLAN Interface will be isolated from other Inband VLAN Interfaces.

**Note**
The IP address of the bridge will be the active IP address of the Inband VLAN Interface as well as of the Out-of-band Ethernet Interface!

### Application

Bridging an Inband VLAN Interface to the Out-of-band Ethernet Interface enables management of all OS900 on the same subnet. This application saves on a customer (data) port.

### Procedure

1. Create an ACL that will cause management packets to be *trapped* to the CPU as follows:

   1.1. Enter **`configure terminal`** mode.

   1.2. Create an ACL by invoking the command:

   **`access-list extended WORD`**

   where,

   **`WORD`**: Name of the ACL (new or existing)

   1.3. Create a rule by invoking the command:

   **`rule RULE_NUM`**

   where,

   **`RULE_NUM`**: Index of rule

   1.4. Invoke the command

   **`action trap-to-cpu [high-priority]`**

   where,

   **`[high-priority]`**: With high priority.
2. Create an Interface Bridge as follows:

2.1. Enter **`configure terminal`** mode.

2.2. Create a bridge by invoking the command:

**`interface bridge BRNAME`**

where,

**`BRNAME`**: Name for a bridge. The format must be **`brX`**, where **`X`** is a numeric (e.g., **`br5`**)

2.3. In the node of the bridge define an IP address for the bridge by invoking the command:

**`ip A.B.C.D/M`**

where,

**`A.B.C.D/M`**: IP address/Mask of the bridge.
The mask can be up to 31 bits long.

2.4. Enable management access via the bridge by invoking the command:

**`management [snmp|telnet|ssh|tftp] [SOURCE_IPV4_ADDRESS]`**

where,

**`snmp`**: Enable SNMP management

**`telnet`**: Enable TELNET management

**`ssh`**: Enable SSH management

**`tftp`**: Enable TFTP server on the OS900 and allow TFTP clients to access configuration files stored in the OS900

**`[SOURCE_IPV4_ADDRESS]`**: IP address of the management host or management subnet (IP address/mask). The mask can be up to 31 bits long.

3. To include the Out-of-band Ethernet Interface in the bridge:

3.1. Enter the mode of the Out-of-band Ethernet Interface by invoking the command:

**`interface out-of-band eth0`**

3.2. Include the Out-of-band Ethernet Interface in the bridge by invoking the command:

**`bridge BR_NAME`**

where,

**`BR_NAME`**: Name of the bridge in which the Inband VLAN Interface is to be included (e.g., **`br5`**).

4. To include the Inband VLAN Interface in the bridge:

4.1. Enter the mode of the Inband VLAN Interface by invoking the command:

**`interface vlan IFNAME`**

where,

**`IFNAME`**: ID of the existing Inband VLAN Interface (e.g., **`vif3`**) to be bridged.

4.2. Include the Inband VLAN Interface in the bridge by invoking the command:

**`bridge BR_NAME`**

where,

**`BR_NAME`**: Name of the bridge in which the Inband VLAN Interface is to be included (e.g., **`br5`**).

4.3. Bind the ACL to the Inband VLAN Interface in the bridge by invoking the command:

**`access-group WORD`**

where,

**`WORD`**: Name of Access List

5. To enable management of each of the other OS900s on the same subnet, on *each* of the other OS900s:

5.1. Create an Inband VLAN Interface with the same ID as that of the OS900 with the bridged interfaces by invoking the command:

**`interface vlan IFNAME`**

where,

**`IFNAME`**: ID of Inband VLAN Interface.

5.2. In the Inband VLAN Interface, include the physical port to which the OS900 with the bridged interfaces is connected.

5.3. Enable management access by invoking the command:

**`management [snmp|telnet|ssh|tftp] [SOURCE_IPV4_ADDRESS]`**

where,

**`[SOURCE_IPV4_ADDRESS]`**: IP address of the management host or management subnet (IP address/mask). The mask can be up to 31 bits long.

## Example

### Purpose

This example demonstrates how to set up three OS900s to be managed via the Out-of-band Ethernet Interface (MGT ETH) of just one OS900. This is done by bridging the Inband VLAN Interface to the Out-of-band Ethernet Interface.

### Network

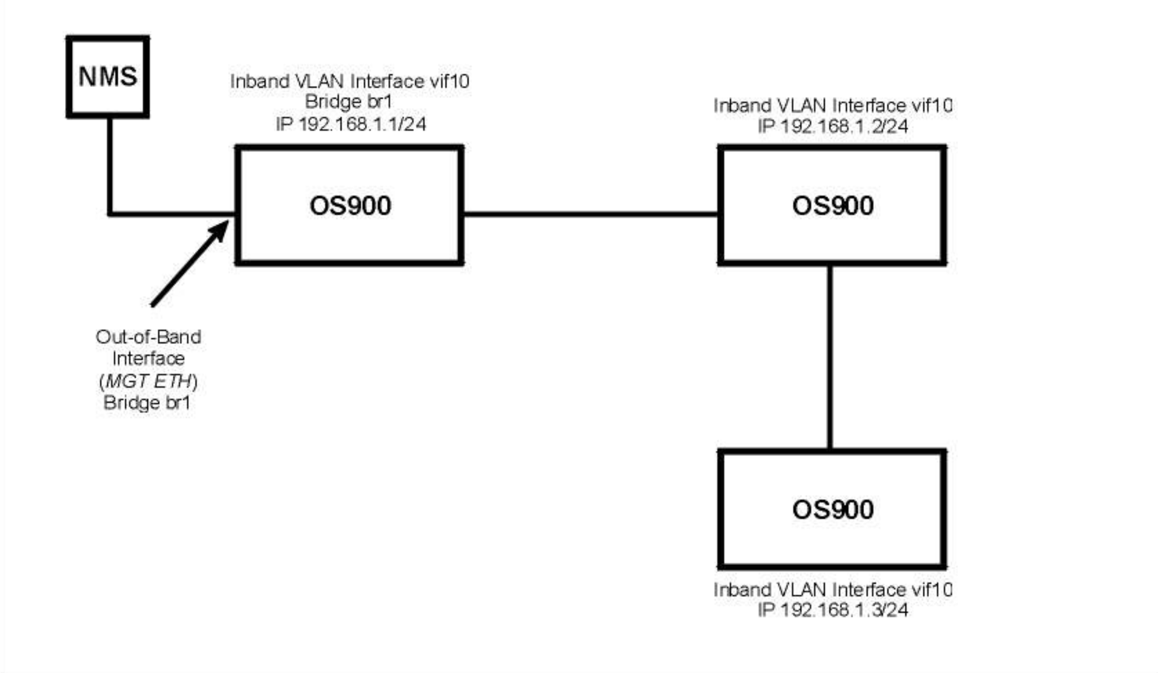



**Figure 20: OS900s to be Managed via one Out-of-band Ethernet Interface**

### Configuration

------------Setting up the OS900 via whose Out-of-band Ethernet Interface mangement is to be performed------------

```
MRV OptiSwitch 910 version 2_1_4
OS910 login: admin
Password:
Last login: Sat Jan  1 00:47:51 2000 on ttyS0

ATTENTION: LOGOUT timeout is set to 13 min.
OS910> enable
OS910# configure terminal
```

```
OS910(config)# access-list extended br1
OS910(config-access-list)# rule 10
OS910(config-rule)# action trap-to-cpu

OS910(config-rule)# exit
OS910(config-access-list)# exit
OS910(config)# interface bridge br1
OS910(config-br1)# ip 192.168.1.1/24
OS910(config-br1)# management

OS910(config-br1)# exit
OS910(config)# interface out-of-band eth0
OS910(config-eth0)# bridge br1

OS910(config-eth0)# exit
OS910(config)# interface vlan vif10
OS910(config-vif10)# tag 10
OS910(config-vif10)# ports 3
Interface is activated.
OS910(config-vif10)# bridge br1
OS910(config-vif10)# access-group br1
OS910(config-vif10)#

-------------------------------------------------------------Setting up the Second OS900-------------------------------------------------------------

MRV OptiSwitch 910 version 2_1_4
OS910 login: admin
Password:
Last login: Sat Jan  1 00:47:51 2000 on ttyS0

ATTENTION: LOGOUT timeout is set to 13 min.
OS910> enable
OS910# configure terminal
OS910(config)# interface vlan vif10
OS910(config-vif10)# tag 10
OS910(config-vif10)# port 3
Interface is activated.
OS910(config-vif10)# ip 192.168.1.2/24
OS910(config-vif10)# management
OS910(config-vif10)#

-------------------------------------------------------------Setting up the Third OS900-------------------------------------------------------------

MRV OptiSwitch 910 version 2_1_4
OS910 login: admin
Password:
Last login: Sat Jan  1 00:47:51 2000 on ttyS0

ATTENTION: LOGOUT timeout is set to 13 min.
OS910> enable
OS910# configure terminal
OS910(config)# interface vlan vif10
OS910(config-vif10)# tag 10
OS910(config-vif10)# port 3
Interface is activated.
OS910(config-vif10)# ip 192.168.1.3/24
OS910(config-vif10)# management
OS910(config-vif10)#
```

# Chapter 8: Multiple-instance Spanning-Tree Protocol (MSTP)

## General

The newest spanning-tree protocol MSTP (IEEE 802.1**s** standard) is implemented in the OS900. MSTP is backward compatible with the spanning-tree protocols STP (IEEE 802.1**d** standard) and RSTP (IEEE 802.1**w** standard) so that the OS900 can be used in a network consisting of devices operating in STP, RSTP, and MSTP.

## Definition

MSTP allows for the creation of multiple MSTIs on a network with network inter-node links that can be shared by any number of MSTIs. An MSTI is a mechanism that creates traffic bridges between devices on a network in the spanning-tree topology[18] while permitting redundant links that it may use as new bridges in the event of a change in the network's topology.

## Purposes

To:

1. Prevent collapse of communication over a network whose topology is changed dynamically.
2. Address the needs of increasingly faster Ethernet networks with mission-critical applications requiring fast convergence/recovery. (The convergence/recovery time is 50 to 200ms, the specific time depending on the network).
3. Maximize traffic flow across a network by optimizing resource utilization (for e.g., by utilizing unused inter-node links).
4. Balance traffic flow across the network.
5. Improve fault tolerance by enabling traffic to flow unaffected in MSTIs even when failure occurs in one or more of the other MSTIs.
6. To identify and exclude each port looped on itself, i.e., each port whose Tx output is connected to its Rx input.

## MSTIs

### General

An MSTI consists of a grouping of VLANs. Up to 64 MSTIs can be created by the user. Each MSTI has the functionality, capabilities, and advantages of RSTP. Traffic belonging to the VLANs of an MSTI flow through the MSTI path, which is constructed by MSTP. Traffic streams of MSTIs flow independently of one another. Accordingly, if, for example, a specific port is in the blocking state for MSTI $I_1$ and not for MSTI $I_2$, traffic with tags of $I_1$ will be blocked at the port while traffic with tags of $I_2$ will be forwarded at the same port.

*Figure 21*, below, shows three active MSTIs on a network. The MSTI paths may be changed by MSTP when a port is blocked for certain VLANs or when a link in the path is broken.

[18] A tree topology ensures that only one path exists between any two endstations on the network. Closed loops are opened and a redundant standby path is made available to traffic in the event that the primary (active) path is disrupted.

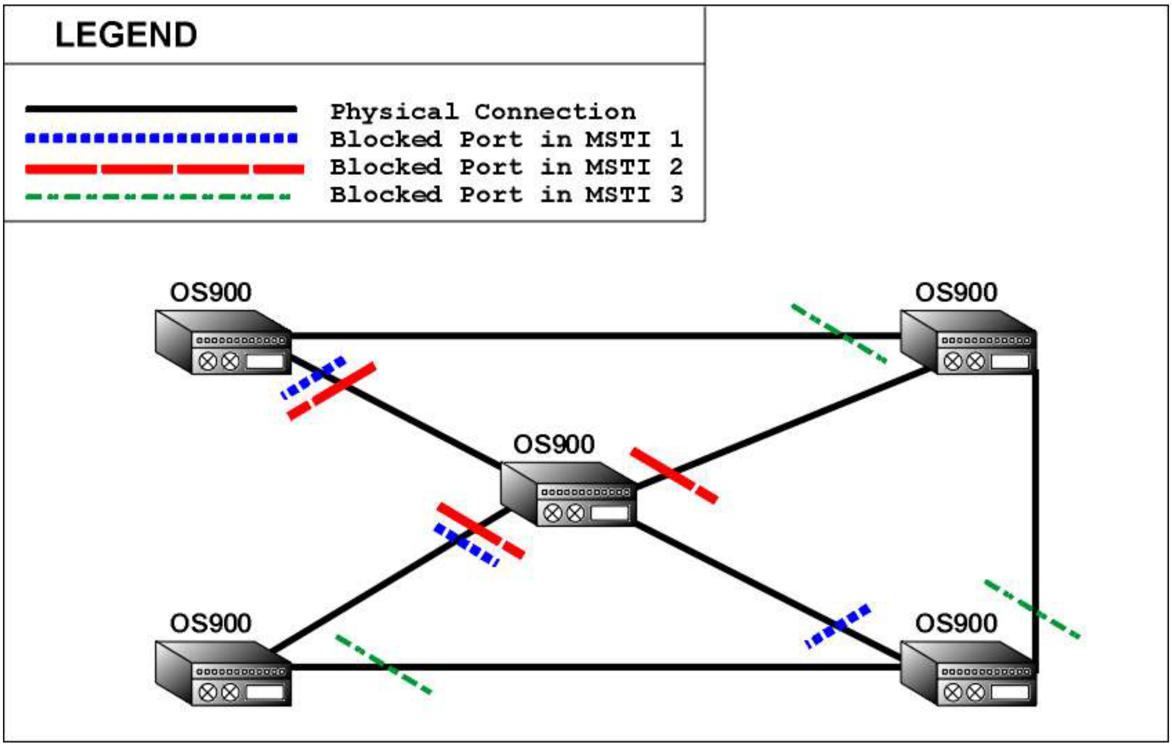



**Figure 21: MSTIs on a Physical Network**

RSTP switches are able to process MSTP BPDUs as if they are RSTP BPDUs. Also, MSTP switches are able to process RSTP BPDUs as if they are MSTP BPDUs. Accordingly, MSTP switches send MSTP BPDUs to RSTP switches, and RSTP switches send RSTP BPDUs to MSTP switches.

However, if an MSTP switch is connected to an STP switch, the MSTP switch sends STP BPDUs to the STP switch.

## Default MSTI

The default MSTI is called CIST (**C**ommon and **I**nternal **S**panning **T**ree). This MSTI is pre-configured and cannot be deleted. All VLANs that are not members of other MSTIs, are members of CIST. Its ID is 0. When VLANs are created, they are automatically included in the CIST. To remove a VLAN from the CIST another MSTI must be created by the user, and the VLAN tag must be moved to this MSTI.

In addition to its role as the default MSTI, CIST interconnects regions and single-instance spanning-tree entities (such as STP and RSTP switches) relating to each region (described in the section *Regions*, page *201*) and STP/RSTP networks as a single virtual bridge.

MSTP uses CIST in creating a spanning tree path interconnecting MST regions and SST[19] entities. In a network of regions and SST entities, each region or SST entity views another region or SST entity that is *directly* connected to it as a *single* spanning-tree bridge. In a region, the SST entity that directly connects to another region is the CIST regional root bridge. One of the CIST regional root bridges is set by MSTP as the CIST root bridge.

[19] SST is STP or RSTP.

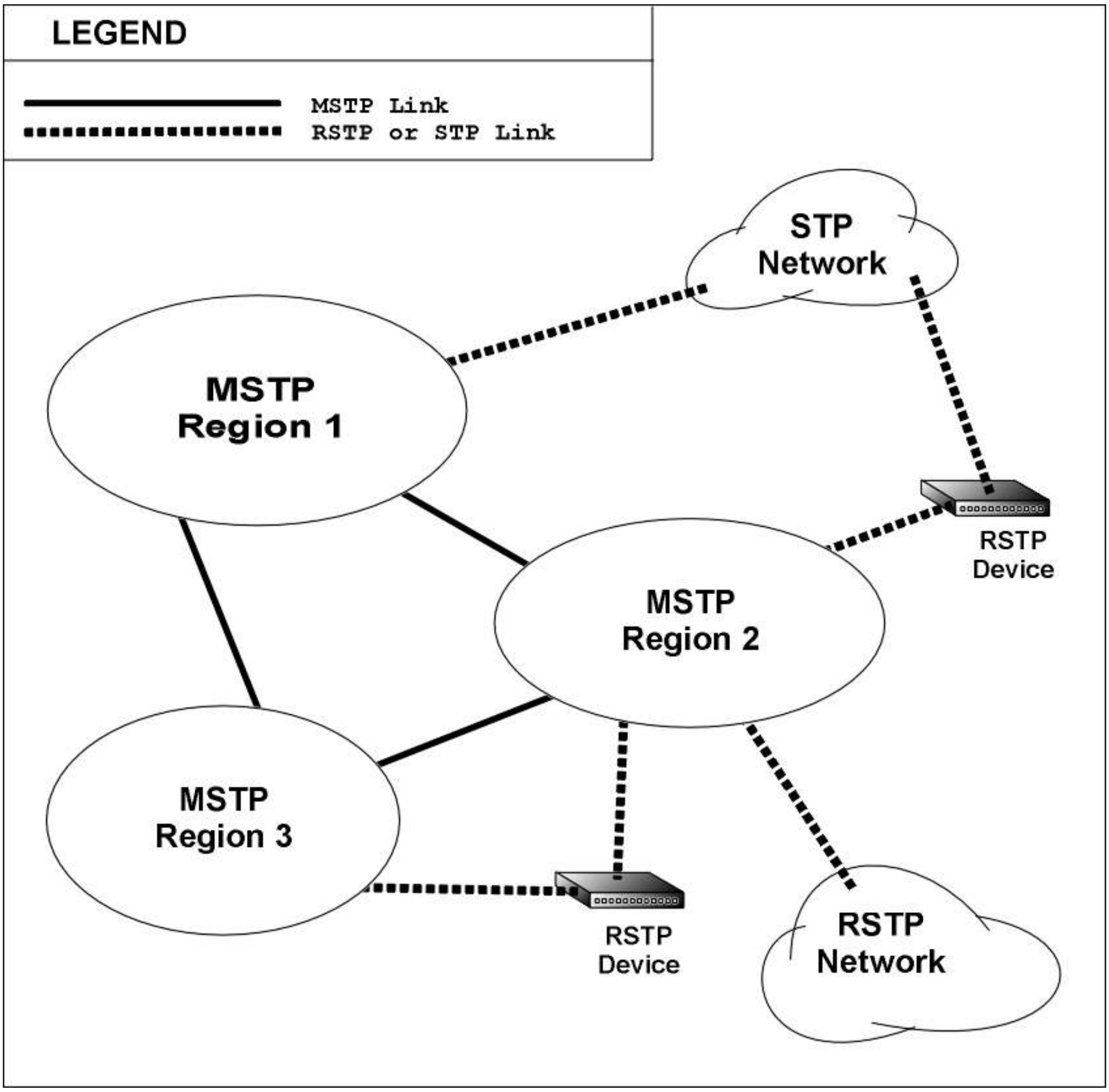



**Figure 22: CIST (Default MSTI) on a Physical Network**

# Regions

A region is a set of interconnected switches all of which have the same values for the following MST parameters:

- Name of the MST region
- Revision number of the current MST configuration (default 0)
- Digest, i.e., VLANs-to-MSTI mappings

> **Note**
>
> A region may include one or more MSTIs as shown in *Figure 23*, page *202*.
>
> Each region is seen as a single bridge by other regions.
>
> In configuring multiple regions, it must be noted that any MSTI in one region is completely independent of any MSTI in another region – even if the MSTIs have the same ID! That is, traffic in one region is directed independently of traffic in another region.

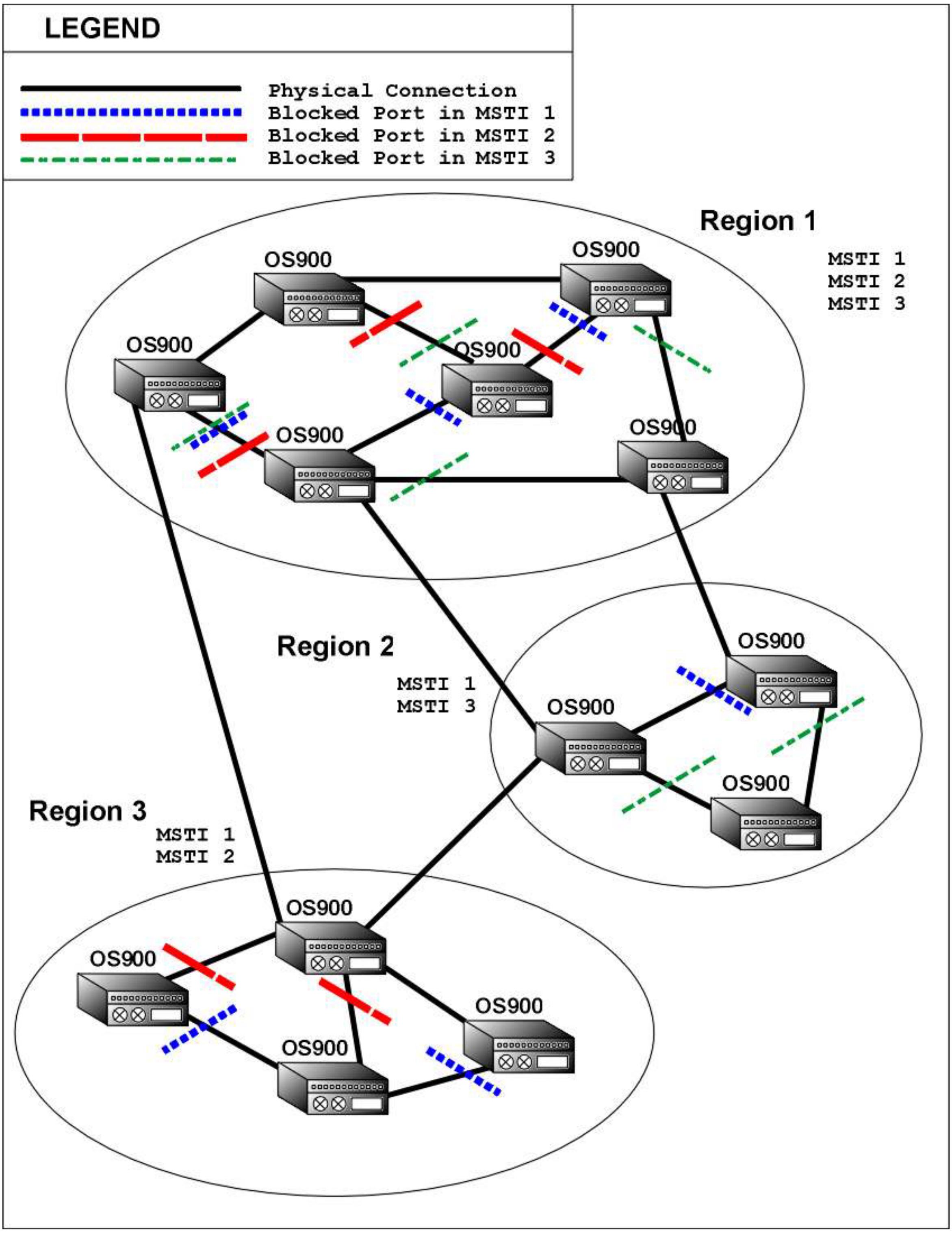



**Figure 23: Regions on a Physical Network**

# Principle of Operation

## Bridge Roles

In MSTP, a switch can have one of the following roles:

**Root Bridge** The bridge that is at the root of a logical tree-topology interconnection of bridges created by the MSTP. The bridge that has the lowest bridge ID in the network is selected as the Root Bridge.

**Designated Bridge** The bridge that can provide the best route to the Root Bridge.

## Port Roles

In MSTP, a port (of a bridge) can have one of the following roles:

**Root Port** The port via which the best route (having the lowest path-cost) is taken to the Root Bridge. The Root Port can be in any of the following states: Forwarding, Learning, or Discarding.

**Designated Port** A port that internally sends/receives to/from the Root Port of the same bridge. Several Designated Ports may exist in an active MSTP configuration. The Designated Port can be in any of the following states: Forwarding, Learning, or Discarding.

**Alternate Port** A port that serves as a standby to the Root Port. In discarding state, the port to which it is linked is always Designated Port. Several Alternate Ports may exist in an active MSTP configuration. The Alternate Port can be only in the following state: Discarding.

**Backup Port** A port that serves as a Backup to the Designated Port. The Backup Port and Designated Port are connected to a device (e.g., hub) that provides traffic sharing on a LAN media segment. The Backup Port can be only in the following state: Discarding.

**Disabled Port** A port that does not participate in MSTP.

## Physical and Active Topologies

*Figure 24*, below, shows a network of interconnected bridges (*physical topology*) participating in MSTP. The *active topology* excludes the direct connection between bridge **B** and **C** and between the Hub and Backup Port.

If any one of the four physical links interconnecting B, C, D, and E, fails MSTP will activate the other three to maintain the requisite spanning-tree bridging topology.

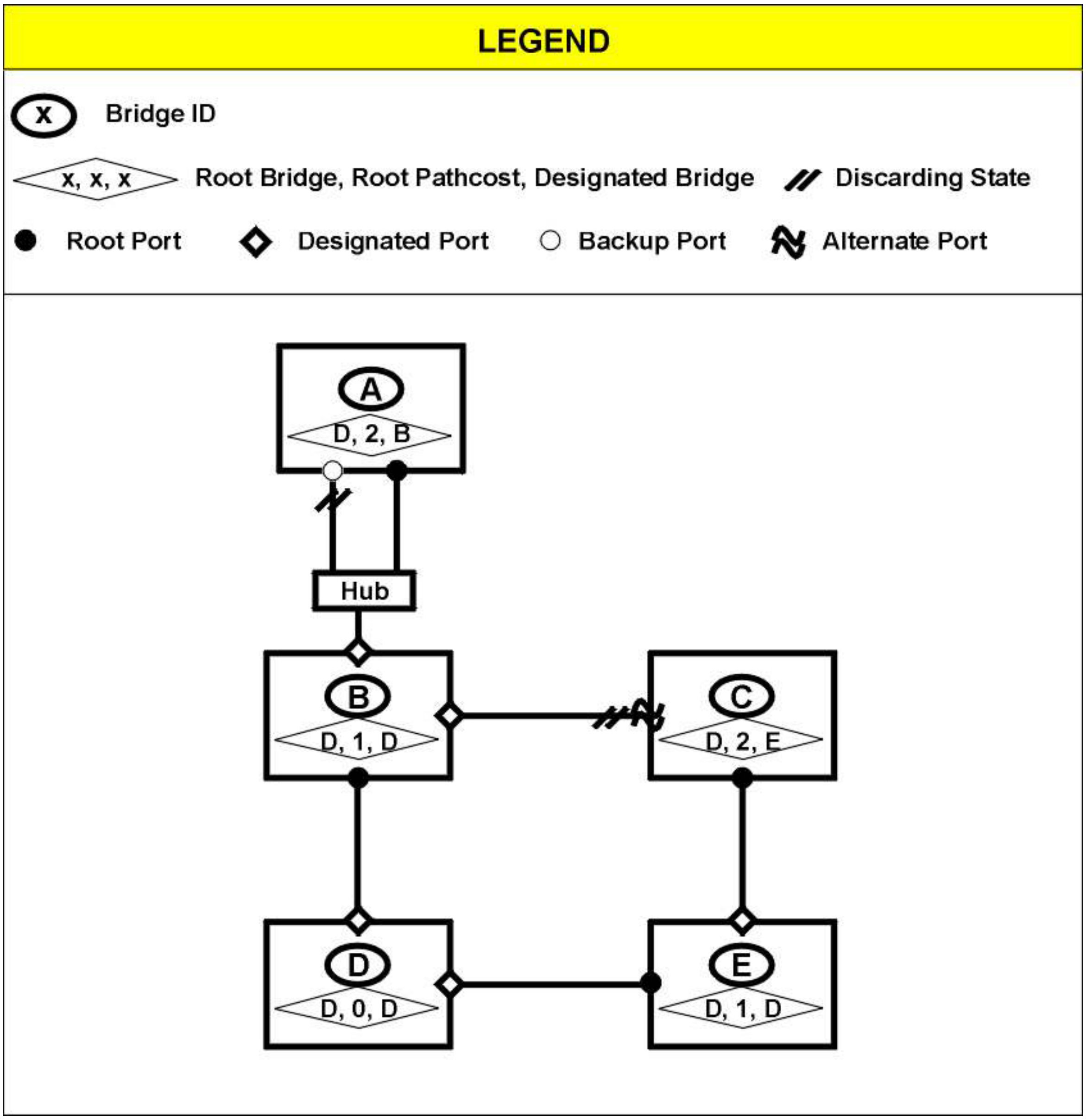



**Figure 24: Network Running MSTP**

# Rules

The following rules apply to MSTP.

1. Up to 64 MSTIs can be created per region.
2. A port can be included in any number of MSTIs.
3. A VLAN can be included in only *one* MSTI.
4. Regions are automatically created if the values of the three region parameters (specified in the section *Regions*, page *201*) are not identical on all the OS900s in the network.
5. A region can include several MSTIs.
6. Traffic in one region is directed independently of traffic in another region.
7. The ID of CIST (default MSTI) is 0 and cannot be changed.
8. A user-created MSTI may be assigned any ID in the range 1 to 64.
9. All VLANs assigned to the same instance will have the same active topology.
10. A network including STP-activated or RSTP-activated switches (in addition to MSTP-activated switches) *must* use CIST.

# Ports

## Placing Restrictions

To place an MSTP-related restriction on specific ports of the OS900:

1. Enter **`spanning-tree`** mode (from **`configure terminal`** mode).
2. Invoke the command:

   **`port PORTS-GROUP (admin-edge|auto-edge|non-stp|root-restricted|tcn-restricted)`**

   where,

   **`PORTS-GROUP`**: Group of Ports to be configured.

   **`admin-edge`**: adminEdge port(s).

   An adminEdge configured port goes directly into the forwarding state upon link establishment.

   For a port participating in STP, AdminEdge = Y causes OperEdge = Y immediately. However, the port starts Forwarding only if no BPDU is received for a period of 2 seconds.

   If a BPDU is received at any time after AdminEdge = Y, OperEdge = N and the port stays in the non-edge mode unless link down/up is performed, whereupon the port reverts to the state for which the whole description above applies again.

   A shortcoming of this method of operation is in the case the following conditions apply: 1) OperEdge = N, 2) the port becomes a Designated port; 3) no agreement is received in response to the proposal within 5 seconds. In this case, the port will forward after a *long* delay; about 3 x Forward Delay time, i.e., 45 seconds.

   **`auto-edge`**: autoEdgePort, per IEEE Std. 802.1D-2004, 14.8.2.3.2.e

   An auto-edge configured port goes directly into the forwarding state upon link establishment.

   For a port participating in STP, AdminEdge = Y causes OperEdge = Y immediately and, unlike in the previous version, the port starts Forwarding *immediately*. Accordingly, this setting should be used only if it is certain that the port is connected only to an end station.

   If it is not connected only to an end station, the port could start forwarding while still in a physical loop with other STP ports, thereby possibly causing broadcast storms.

   In the present version, a new parameter, AutoEdge[20], has been made available. Its purpose is to speed up recovery/convergence of STP bridging that includes a Designated port for which OperEdge = N. As a designated non-edge port, wanting to start forwarding, it sends a proposal flag. If it does not receive an agreement within 5 seconds (2 seconds + migration time), and AutoEdge = Y, it decides, that it is OperEdge = Y and starts forwarding immediately. If AutoEdge = N, the delay in forwarding could be as much as 3 x Forwarding Delay Time.

   **`non-stp`**: Port(s) not to participate in MSTP

   **`root-restricted`**:A Boolean value set by management. If TRUE causes the Port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be FALSE by default. If set, it can prevent full spanning tree connectivity. It is set by the network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, for possibly the reason that the bridges are not under the full control of the administrator.

[20] According to the bridge-detection machine Draft 802.1D-2400.

**tcn-restricted**: A Boolean value set by management. If TRUE causes the Port not to propagate received topology change notifications and topology changes to other Ports, e.g., Topology Change Notifications (TCNs) and Topology Changes (TCs). This parameter should be FALSE by default. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent incorrectly learnt station location information. It is set by a network administrator to prevent bridges external to a core region of the network causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or MAC_Operational for the attached LANs transitions frequently.

## Removing Restrictions

To remove the administrator-imposed MSTP-related restriction on specific ports of the OS900:

1. Enter **spanning-tree** mode.
2. Invoke the command:
   **no port PORTS-GROUP (admin-edge|auto-edge|non-stp|root-restricted|tcn-restricted)**

# BPDU Storm Guard

## General

The storm guard is a mechanism used to notify and, optionally, isolate (disable) a port that receives BPDUs at a rate that is in excess of the set limit. By default, this limit is 25 BPDUs per second (for any port).

## Custom

To set a new BPDU rate for ports:

1. Enter **spanning-tree** mode.
2. Invoke the command:
   **bpdu-storm-guard <0-1000> (inform|isolate)**
   
   **<1-1000>**: Range of rates (number of BPDUs per second) from which one is to be selected. Default: 25 BPDUs per second.
   
   **inform**: Notify which ports transmit BPDUs in excess of the set limit.
   
   **isolate**: Notify which ports transmit BPDUs in excess of the set limit and isolate (disable) them. (Default).

## Default

To set the storm guard limit to the default value (25 BPDUs per second):

1. Enter **spanning-tree** mode.
2. Invoke the command:
   **no bpdu-storm-guard**

## Disabling

To disable the storm guard, i.e., to remove the limit on the rate for BPDUs:

1. Enter **spanning-tree** mode.
2. Invoke the command:
   **bpdu-storm-guard 0**

To reconnect one or more ports isolated by the storm guard to the network, following the procedure given in the section *Reconnecting Isolated Ports*, page *151*:

# Applications

This section presents three typical MSTI applications in networks to show the scope of MSTP. They are:

– Single MSTI
– Multiple MSTIs without Load Balancing
– Multiple MSTIs *with* Load Balancing

## Single MSTI

### General

In this application, the default MSTI (*CIST*) is used to interconnect the whole network. Only the single command **`enable`** needs to be invoked to actively sustain the spanning tree topology for the entire network.

### Example

*Figure 25*, below, shows a network using CIST to interconnect OS900s. A network with a simple topology has been intentionally selected to make it easier to understand the application. In one of several possible active CIST configurations, port blocking prevents traffic flow on the link between OS900 C and OS900 D. However, traffic can flow on all the other links. OS900 A is shown as the current *CIST* Root Bridge.

If any inter-node link (other than that between OS900 C and OS900 D ) fails, the port at OS900 C changes its state from 'blocking' to 'forwarding' in order to rebridge all four nodes.

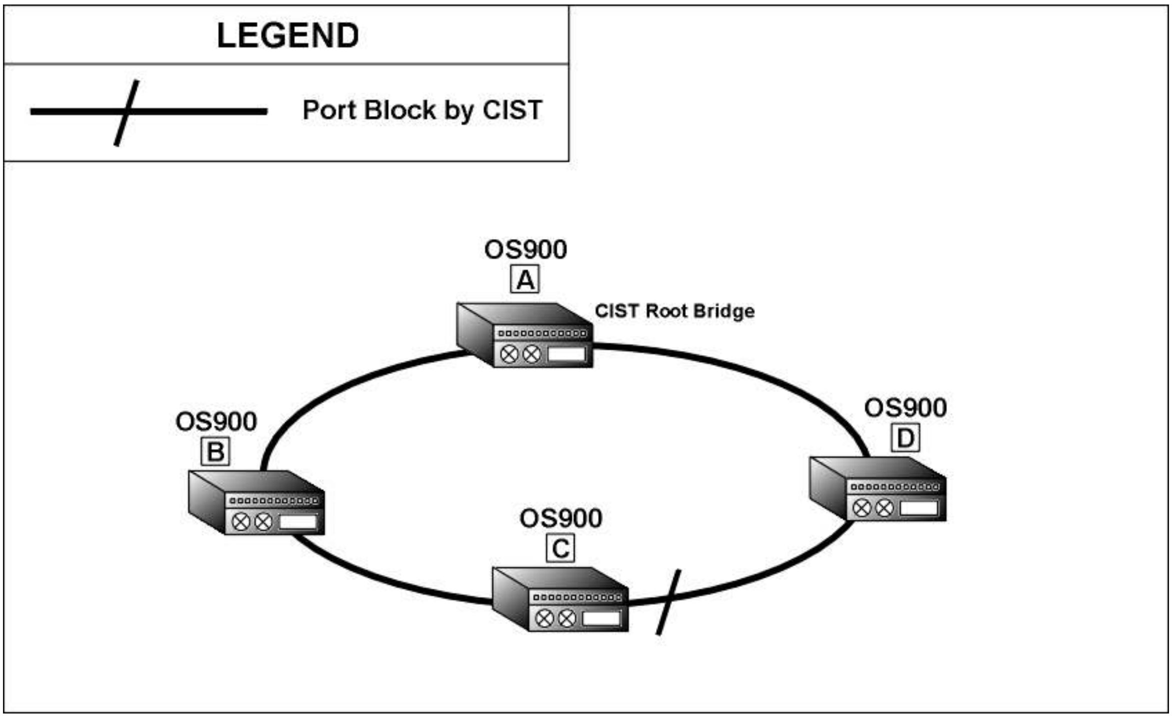



**Figure 25: CIST-configured Network**

### Configuration Procedure

To use CIST to interconnect the switches of a network, simply invoke the following command:

**`enable`**

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# spanning-tree
OS900(config-mstp) enable
```

The command enables MSTP, which prevents traffic flow between OS900 C and OS900 D. A spanning tree is configured on the network according to default values (e.g., bridge priority, port pathcost, etc.). CIST is the only active MSTI and includes all VLANs.

#### Viewing

To view which ports are blocking and which are forwarding, invoke the command:

```
show spanning-tree port 1-2
```

To view which OS900 is the root bridge, invoke the command:

```
show spanning-tree instance 0
```

> **Note**
> By default, the port on the OS900 that has the longest distance to the root is blocked.

### Multiple MSTIs *without* Load Balancing

#### General

In this application, multiple MSTIs (each having several VLANs) are applied to a network *without* utilizing the traffic load balancing capability of multiple MSTIs.

#### Example

*Figure 26*, below, shows a network built with four OS900s:
OS900 A, OS900 B, OS900 C, and OS900 D.

On each OS900, four interfaces (VLANs) are configured: **`vif1`**, **`vif2`**, **`vif3`**, and **`vif4`**.

**`vif1`** is assigned tag **`110`**. **`vif2`** is assigned tag **`120`**. **`vif3`** is assigned tag **`130`**. **`vif4`** is assigned tag **`140`**.

Two MSTIs are configured on each of the OS900s: **`1`** and **`2`**.

MSTI **`1`** contains the interfaces `vif1` and `vif2`, and serves as a pathway for traffic on these interfaces. MSTI **`2`** contains the interfaces `vif3` and `vif4`, and serves as a pathway for traffic on these interfaces.

By default, the OS900 with lowest MAC address is set as the root bridge by MSTP. Since the two MSTIs **`1`** and **`2`** are configured on all the OS900s in the network, the OS900 with the lowest MAC address is set as the common root bridge for the MSTIs. OS900 A is shown as the common root bridge. In one of several possible active MSTI **`1`** or MSTI **`2`** configurations, the link between OS900 A and OS900 D is blocked for all traffic. As a result, both MSTI **`1`** and MSTI **`2`** traffic entering OS900 A is directed over the same link (between OS900 A and OS900 B).

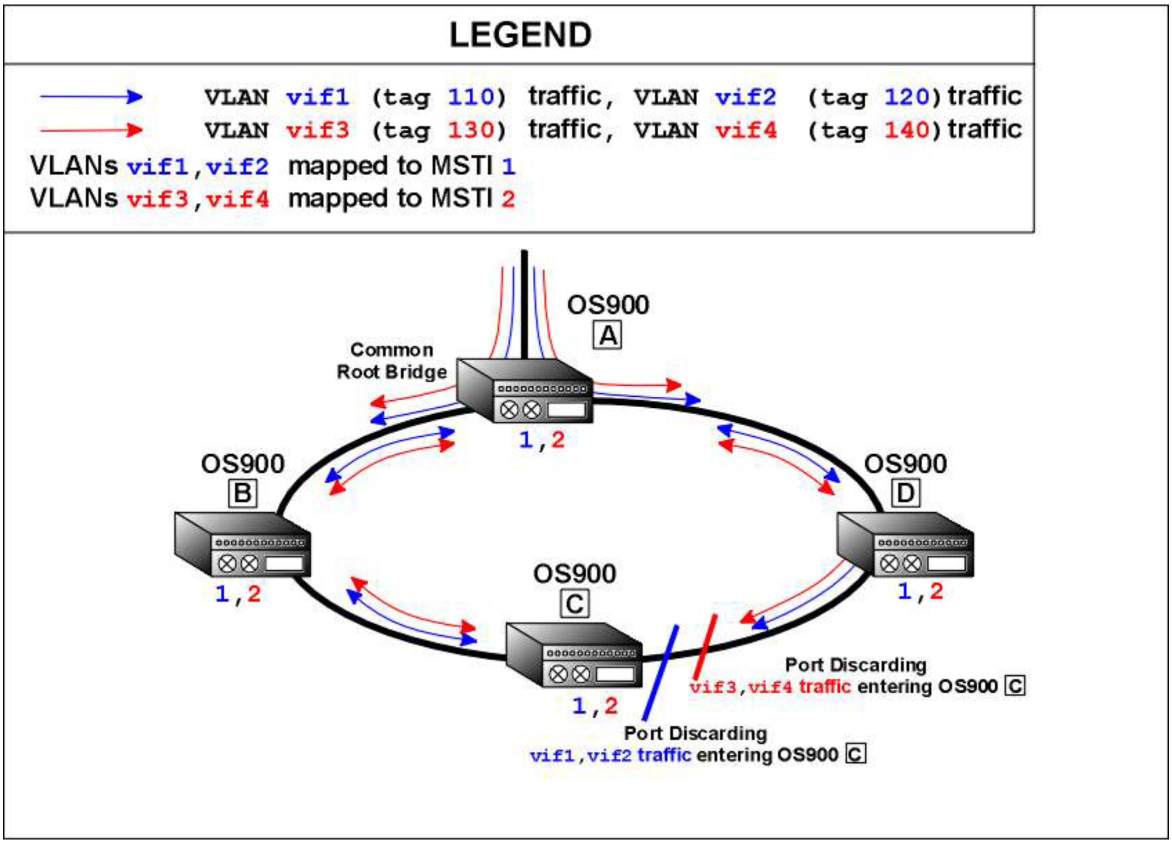



**Figure 26: Multiple-MSTI Network *without* Load Balancing**

### Configuration Procedure

The procedure for configuring multiple MSTIs on OS900s *without* traffic load balancing is described using the network in *Figure 26* as an example.

1. Create the interfaces (VLANs, i.e., **vif1**, **vif2**, **vif3**, and **vif4**) to be included in MSTIs using either of the following commands, once for each interface:

   For Tag-based, Non-IP type interfaces[21]

   **interface vlan IFNAME**

   where,

   **vlan**: VLAN

   **IFNAME**: Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095

   Example

```
OS900> enable
OS900# configure terminal

OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 1
OS900(config-vif1)# tag 110
Interface is activated.
OS900(config-vif1)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 2
OS900(config-vif2)# tag 120
Interface is activated.
OS900(config-vif2)# exit
```

[21] A tag-based interface has a unique IEEE 802.1Q VLAN ID. A Non-IP type interface has no IP address.

```
OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 3
OS900(config-vif3)# tag 130
Interface is activated.
OS900(config-vif3)# exit

OS900(config)# interface vlan vif4
OS900(config-vif4)# ports 4
OS900(config-vif4)# tag 140
Interface is activated.
OS900(config-vif4)#
```

2. Enter the spanning-tree mode using the command:
   **`spanning-tree`**

   Example

```
OS900(config-vif4)# exit
OS900(config)# spanning-tree
OS900(config-mstp)#
```

3. Create MSTIs using the command:
   **`instance <0-64> vlan TAGS-LIST`**

   where,

   **`instance`**: MSTI

   **`<0-64>`**: Range of valid MSTI IDs from which one ID is to be selected.

   **`vlan`**: VLANs are to be mapped to the MSTI.

   **`TAGS-LIST`**: List of VLAN tags to be members of the specific MSTI.

   Example

```
OS900(config-mstp)# instance 1 vlan 110,120
OS900(config-mstp)# instance 2 vlan 130,140
OS900(config-mstp)#
```

   (To delete the instance, invoke the command **`no instance <1-64> vlan TAGS-LIST`**.)

4. Enable MSTP for the OS900 using the command:
   **`enable`**

   Example

```
OS900(config-mstp) enable
OS900(config-mstp)#
```

5. Repeat Steps *1* to *4* above for each OS900.

### Viewing

To view which ports are blocking and which are forwarding, invoke the command:

**`show spanning-tree port 1-2`**

To view which OS900 is the root bridge, invoke the commands:

**`show spanning-tree instance 1`**

**`show spanning-tree instance 2`**

| | |
|---|---|
| | **Note**<br>By default, the port on the OS900 that has the longest distance to the root is blocked. |

## Multiple MSTIs *with* Load Balancing

### General

In this application, multiple MSTIs (each having several VLANs) are applied to a network utilizing the traffic load balancing capability of multiple MSTIs.

### Example

*Figure 27*, below, shows a network built with four OS900s:

OS900 A, OS900 B, OS900 C, and OS900 D.

On each OS900, four interfaces (VLANs) are configured: **vif1**, **vif2**, **vif3**, and **vif4**.

**vif1** is assigned tag **110**. **vif2** is assigned tag **120**. **vif3** is assigned tag **130**. **vif4** is assigned tag **140**.

Two MSTIs are configured on each of the OS900s: **1** and **2**.

MSTI **1** contains the interfaces vif1 and vif2, and serves as a pathway for traffic on these interfaces. MSTI **2** contains the interfaces vif3 and vif4, and serves as a pathway for traffic on these interfaces.

*Bridge priority* is configured for each instance on the OS900s (using the command **instance INSTANCE_ID priority NUMBER** in the mode **spanning-tree**). The two OS900s with the lowest bridge priority in each MSTI are set as the root bridge by MSTP. OS900 B is shown as the root bridge in MSTI **1**. OS900 D is shown as the root bridge in MSTI **2**. In one of several possible active MSTI **1** or MSTI **2** configurations, vif1 and vif2 traffic entering OS900 A is directed on the link between OS900 A and OS900 B while vif3 and vif4 traffic entering OS900 A is directed on the link between OS900 A and OS900 D. That is, MSTI **1** and MSTI **2** traffic is divided between links. Thus, load balancing of traffic entering OS900 A is achieved.

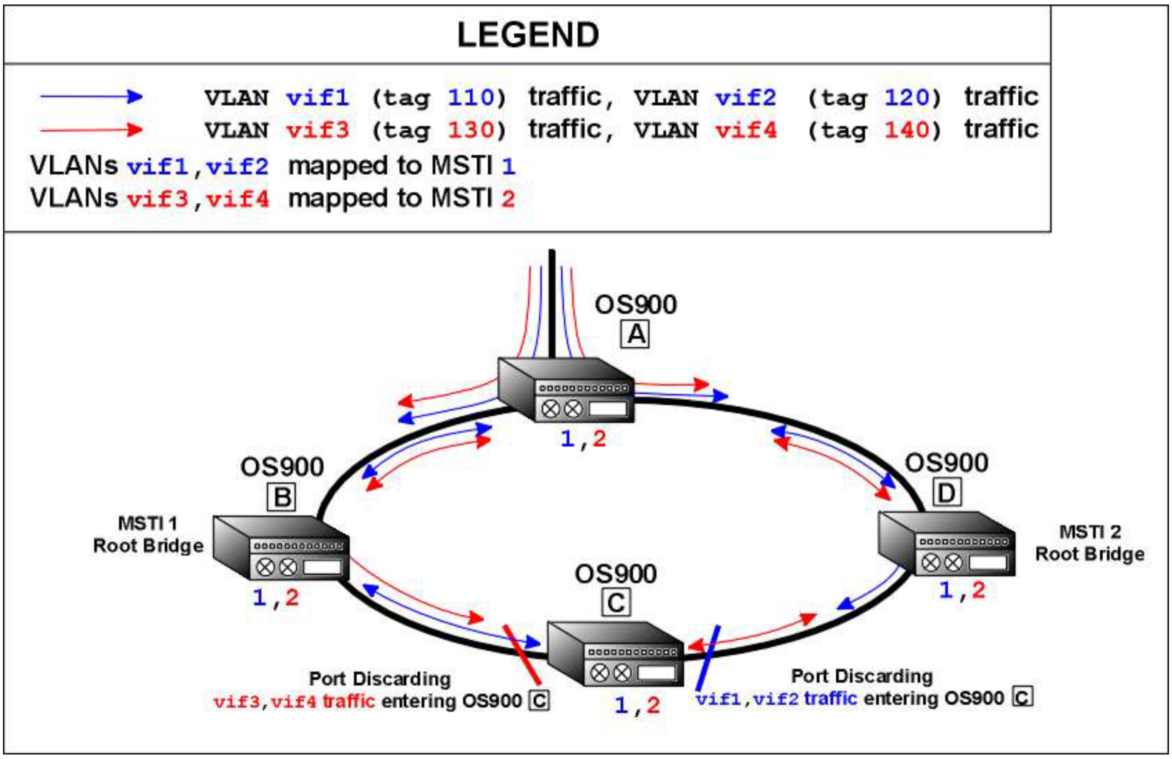



**Figure 27: Multiple-MSTI Network *with* Load Balancing**

### Configuration Procedure

The procedure for configuring multiple MSTIs on OS900s *with* traffic load balancing is described using the network in *Figure 27* as an example.

1. Create the interfaces (VLANs, i.e., **`vif1`**, **`vif2`**, **`vif3`**, and **`vif4`**) to be included in MSTIs as follows, noting that the assignment of IP address is optional since it is not required for MSTIs:

    a. Invoke the commands: **`interface vlan vif1`**, **`ports 1`**, **`tag 110`**, and **`ip 20.30.30.34/24`**.

    b. Invoke the commands: **`interface vlan vif2`**, **`ports 2`**, **`tag 120`**, and **`ip 60.10.10.10/24`**.

    c. Invoke the commands: **`interface vlan vif3`**, **`ports 3`**, **`tag 130`**, and **`ip 70.30.30.34/24`**.

    d. Invoke the commands: **`interface vlan vif2`**, **`ports 4`**, **`tag 140`**, and **`ip 80.30.30.34/24`**.

    Example

```
OS900> enable
OS900# configure terminal

OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 1
OS900(config-vif1)# tag 110
Interface is activated.
OS900(config-vif4)# ip 20.30.30.34/24
OS900(config-vif1)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 2
OS900(config-vif2)# tag 120
Interface is activated.
OS900(config-vif4)# ip 60.10.10.10/24
OS900(config-vif2)# exit

OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 3
OS900(config-vif3)# tag 130
Interface is activated.
OS900(config-vif4)# ip 70.30.30.34/24
OS900(config-vif3)# exit

OS900(config)# interface vlan vif4
OS900(config-vif4)# ports 4
OS900(config-vif4)# tag 140
Interface is activated.
OS900(config-vif4)# ip 80.30.30.34/24
OS900(config-vif4)#
```

2. Enter the spanning-tree mode using the command:
    **`spanning-tree`**

    Example

```
OS900(config-vif4)# exit
OS900(config)# spanning-tree
OS900(config-mstp)#
```

3. Create MSTIs using the command:
    **`instance <0-64> vlan TAGS-LIST`**
    where,
    **`instance`**: MSTI
    **`<0-64>`**: Range of valid MSTI IDs from which one ID is to be selected.

**vlan**: VLANs are to be mapped to the MSTI.

**TAGS-LIST**: List of VLAN tags to be members of the specific MSTI.

Example

```
OS900(config-mstp)# instance 1 vlan 110,120
OS900(config-mstp)# instance 2 vlan 130,140
OS900(config-mstp)#
```

(To delete the instance, invoke the command **no instance <1-64> vlan TAGS-LIST**.)

4. Set the *bridge priority* using the command:

   **instance <0-64> priority NUMBER**

   where,

   **instance**: MSTI

   **<0-64>** Range of valid MSTI IDs from which one ID is to be selected.

   **priority**: Bridge priority of the OS900.

   **NUMBER**: Value of the priority. Any value in the range <0-61440> may be selected provided it is a multiple 4096.

Example

```
OS900(config-mstp)# instance 1 priority 4096
accepted: dec=4096 or hex=0x1000
OS900(config-mstp)#
```

> **Note**
>
> For example, in *Figure 27*, page *211*, to make OS900 B the root bridge of MSTI **1**, set its bridge priority to the lowest among the other OS900s for MSTI **1**.
>
> To make OS900 D the root bridge of MSTI **2**, set its bridge priority to the lowest among the other OS900s for MSTI **2**.

5. Enable MSTP for the OS900 using the command:

   **enable**

Example

```
OS900(config-mstp) enable
OS900(config-mstp)#
```

6. Repeat Steps *1* to 5 above for each OS900.

# Optional Configuration Parameters

## Port Priority

To set the *port priority*, invoke the command:

**instance <0-64> port PORTS-GROUP priority NUMBER**

where,

**instance**: MSTI

**<0-64>**: Range of valid MSTI IDs from which one ID is to be selected.

**port**: Port configuration.

**PORTS-GROUP**: Group of Ports.

**priority**: Bridge priority of the OS900.

**NUMBER**: Value of the priority. Any value in the range <0-240> may be selected provided it is a multiple 16.

Example:

```
OS900(config-mstp)# instance 1 port 1-3 priority 80
OS900(config-mstp)#
```

## Port Path Cost

To set the *port path cost*[22], invoke the command:

**instance <0-64> port PORTS-GROUP path-cost NUMBER|auto**

where,

**instance**: MSTI

**<0-64>**: Range of valid MSTI IDs from which one ID is to be selected.

**port**: Port configuration.

**PORTS-GROUP**: Group of Ports.

**path-cost**: Port path cost of the OS900.

**NUMBER**: Value of the priority. Any value in the range 1-200000000 may be selected.

**auto**: Automatic setting of port path cost.

Example:

```
OS900(config-mstp)# instance 1 port 1-3 path-cost 800000
OS900(config-mstp)#
```

## Region Name

A region name may be assigned to an MST *either* in alphanumeric *or* in hexadecimal format.

### Assigning

#### *Alphanumeric Format*

To assign a region name in alphanumeric format to the MST, invoke the command:

**name WORD**

where,

**WORD**: MST region name in alphanumeric format

#### *Hexadecimal Format*

To assign a region name in hexadecimal format to the MST, invoke the command:

**hex-name HEXWORD**

where,

**WORD**: MST region name in hexadecimal format

### Removing

#### *Alphanumeric Format*

To remove a region name in alphanumeric format of the MST, invoke the command:

**no name [WORD]**

where,

**[WORD]**: MST region name alphanumeric format

#### *Hexadecimal Format*

To remove a region name in hexadecimal format of the MST, invoke the command:

**no hex-name [HEXWORD]**

where,

**[WORD]**: MST region name alphanumeric format

[22] A port having a higher speed has a lower pathcost. Accordingly, as a rule, a port trunk (see ***Chapter 13:*** *IEEE 802.3ad Link Aggregation (LACP)*, page *273*) has a lower pathcost than a single port.

## Revision

### Assigning

To assign a revision number to the MST, invoke the command:

**`revision <0-65535>`**

where,

`<0-65535>`: MST revision number

### Removing

To remove the revision number of the MST, invoke the command:

**`no revision`**

## Forward Delay Time

### Changing

The default time spent in the listening and learning state is 15 seconds.

To change this time, invoke the command:

**`forward-time <4-30>`**

where,

`<4-30>`: Listening and learning time in the range 4 to 30 seconds.

### Default

To revert to the default listening and learning time (15 seconds), invoke the command:

**`no forward-time`**

## Hello Time

### Changing

The default time between each BPDU sent on a port is 2 seconds.

To change this time, invoke the command:

**`hello-time <1-10>`**

where,

`<1-10>`: Inter-BPDU time interval in the range 1 to 10 seconds.

### Default

To revert to the default hello time (2 seconds), invoke the command:

**`no hello-time`**

## Maximum Age

### Changing

The default wait time for a bridge port before saving its configuration BPDU information is 20 seconds.

To change this time, invoke the command:

**`max-age <6-40>`**

where,

`<6-40>`: Wait time in the range 6 to 40 seconds.

### Default

To revert to the default wait time (20 seconds), invoke the command:

**`no max-age`**

## Maximum Hops

The maximum number of hops in the region. The MSTI root bridge sends BPDUs with the hop count set to the maximum value. When a bridge receives this BPDU, it decrements the hop count by one in the BPDU and then forwards the BPDU. When a bridge receives a BPDU with a hop count of zero, the bridge discards the BPDU.

### Changing

The default maximum number of hops is 14.

To change this number, invoke the command:

**`max-hops <4-60>`**

where,

**`<6-40>`**: Maximum number of hops in the range 6 to 40 seconds.

### Default

To revert to the default maximum number of hops (14), invoke the command:

**`no max-hops`**

## Tagged BPDUs

### Ingress

#### *Flood or Drop*

To cause ingress BPDUs with certain tags to be dropped or to be flooded to all member ports of a VLAN, invoke the command:

**`tagged-bpdu-ports PORTS-GROUP rx TAG-LIST (drop|flood)`**

where,

**`PORTS-GROUP`**: Group of ports for which ingress BPDUs are to be dropped or flooded to member ports of VLANs to which they belong.

**`TAG-LIST`**: List of VLAN tags such that BPDUs possessing them are to be dropped or flooded.

**`drop`**: Drop BPDUs.

**`flood`**: Flood BPDUs to all member ports of a VLAN.

#### *Canceling*

To cancel handling of BPDUs according to the ***Flood or Drop*** setting described in the section above, invoke the command:

**`no tagged-bpdu-ports PORTS-GROUP rx TAG-LIST (drop|flood)`**

where,

**`PORTS-GROUP`**: Group of ports for which ingress BPDUs are to be dropped or flooded.

**`TAG-LIST`**: List of VLAN tags such that BPDUs possessing them are to be handled independently of the setting described in the section ***Flood or Drop***.

**`drop`**: BPDUs that were set to be dropped.

**`flood`**: BPDUs that were set to be flooded.

### Egress

#### *Adding*

To add a VLAN tag to egress BPDUs, invoke the command:

**`tagged-bpdu-ports PORTS-GROUP tx TAG`**

where,

**`PORTS-GROUP`**: Group of ports whose egress BPDUs are to be tagged.

**`TAG`**: VLAN tag to be assigned to egress BPDUs.

***Deleting***

To delete the VLAN tag set to be added to egress BPDUs, invoke the command:

**no tagged-bpdu-ports PORTS-GROUP tx TAG**

where,

**PORTS-GROUP**: Group of ports whose egress BPDUs are to be tagged.

**TAG**: VLAN tag to be assigned to egress BPDUs.

# Configuration Example

The following example shows how to configure the OS900s in the network of *Figure 27* for traffic load balancing.

### OS900 A Configuration

```
MRV OptiSwitch 910 version d1734-22-09-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
OS900(config)# interface vlan ?
  IFNAME  Interface device-name as vif# (i.e vif3 )
OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 1
OS900(config-vif1)# tag 110
Interface is activated.
OS900(config-vif1)# ip 20.30.30.35/24
OS900(config-vif1)# name Jojo1
OS900(config-vif1)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 2
OS900(config-vif2)# tag 120
Interface is activated.
OS900(config-vif2)# ip 60.10.10.11/24
OS900(config-vif2)# name Jojo2
OS900(config-vif2)# exit

OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 3
OS900(config-vif3)# tag 130
Interface is activated.
OS900(config-vif3)# ip 70.30.30.35/24
OS900(config-vif3)# name Jojo3
OS900(config-vif3)# exit

OS900(config)# interface vlan vif4
OS900(config-vif4)# ports 4
OS900(config-vif4)# tag 140
Interface is activated.
OS900(config-vif4)# ip 80.30.30.35/24
OS900(config-vif4)# name Jojo4
OS900(config-vif4)# exit

OS900(config)# spanning-tree
OS900(config-mstp)# instance 1 priority 16384
accepted: dec=4096 or hex=0x1000
OS900(config-mstp)# instance 2 priority 20480
accepted: dec=8192 or hex=0x2000
OS900(config-mstp)# instance 1 port 1 priority 64
OS900(config-mstp)# instance 1 port 2 priority 80
OS900(config-mstp)# instance 1 port 1-4 path-cost auto
```

```
OS900(config-mstp)# instance 2 port 1-4 path-cost auto
OS900(config-mstp)# enable
OS900(config-mstp)#
```

## OS900 B Configuration

```
MRV OptiSwitch 910 version d1734-22-09-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
OS900(config)# interface vlan ?
  IFNAME  Interface device-name as vif# (i.e vif3 )
OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 1
OS900(config-vif1)# tag 110
Interface is activated.
OS900(config-vif1)# ip 20.30.30.34/24
OS900(config-vif1)# name Zorro1
OS900(config-vif1)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 2
OS900(config-vif2)# tag 120
Interface is activated.
OS900(config-vif2)# ip 60.10.10.10/24
OS900(config-vif2)# name Zorro2
OS900(config-vif2)# exit

OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 3
OS900(config-vif3)# tag 130
Interface is activated.
OS900(config-vif3)# ip 70.30.30.34/24
OS900(config-vif3)# name Zorro3
OS900(config-vif3)# exit

OS900(config)# interface vlan vif4
OS900(config-vif4)# ports 4
OS900(config-vif4)# tag 140
Interface is activated.
OS900(config-vif4)# ip 80.30.30.34/24
OS900(config-vif4)# name Zorro4
OS900(config-vif4)# exit

OS900(config)# spanning-tree
OS900(config-mstp)# instance 1 priority 4096
accepted: dec=4096 or hex=0x1000
OS900(config-mstp)# instance 2 priority 8192
accepted: dec=8192 or hex=0x2000
OS900(config-mstp)# instance 1 port 1 priority 16
OS900(config-mstp)# instance 1 port 2 priority 32
OS900(config-mstp)# instance 1 port 1-4 path-cost auto
OS900(config-mstp)# instance 2 port 1-4 path-cost auto
OS900(config-mstp)# enable
OS900(config-mstp)#
```

## OS900 C Configuration

```
MRV OptiSwitch 910 version d1734-22-09-05
OS900 login: admin
Password:
```

```
OS900> enable
OS900# configure terminal
OS900(config)# interface vlan ?
  IFNAME  Interface device-name as vif# (i.e vif3 )
OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 1
OS900(config-vif1)# tag 110
Interface is activated.
OS900(config-vif1)# ip 20.30.30.33/24
OS900(config-vif1)# name Lupo1
OS900(config-vif1)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 2
OS900(config-vif2)# tag 120
Interface is activated.
OS900(config-vif2)# ip 60.10.10.9/24
OS900(config-vif2)# name Lupo2
OS900(config-vif2)# exit

OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 3
OS900(config-vif3)# tag 130
Interface is activated.
OS900(config-vif3)# ip 70.30.30.33/24
OS900(config-vif3)# name Lupo3
OS900(config-vif3)# exit

OS900(config)# interface vlan vif4
OS900(config-vif4)# ports 4
OS900(config-vif4)# tag 140
Interface is activated.
OS900(config-vif4)# ip 80.30.30.33/24
OS900(config-vif4)# name Lupo4
OS900(config-vif4)# exit

OS900(config)# spanning-tree
OS900(config-mstp)# instance 1 priority 20480
accepted: dec=4096 or hex=0x1000
OS900(config-mstp)# instance 2 priority 24576
accepted: dec=8192 or hex=0x2000
OS900(config-mstp)# instance 1 port 1-3 priority 80
OS900(config-mstp)# instance 1 port 4 priority 96
OS900(config-mstp)# instance 1 port 1-4 path-cost auto
OS900(config-mstp)# instance 2 port 1-4 path-cost auto
OS900(config-mstp)# enable
OS900(config-mstp)#
```

## OS900 D Configuration

```
MRV OptiSwitch 910 version d1734-22-09-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
OS900(config)# interface vlan ?
  IFNAME  Interface device-name as vif# (i.e vif3 )
OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 1
OS900(config-vif1)# tag 110
Interface is activated.
OS900(config-vif1)# ip 20.30.30.33/24
```

```
OS900(config-vif1)# name Lupo1
OS900(config-vif1)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 2
OS900(config-vif2)# tag 120
Interface is activated.
OS900(config-vif2)# ip 60.10.10.9/24
OS900(config-vif2)# name Lupo2
OS900(config-vif2)# exit

OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 3
OS900(config-vif3)# tag 130
Interface is activated.
OS900(config-vif3)# ip 70.30.30.33/24
OS900(config-vif3)# name Lupo3
OS900(config-vif3)# exit

OS900(config)# interface vlan vif4
OS900(config-vif4)# ports 4
OS900(config-vif4)# tag 140
Interface is activated.
OS900(config-vif4)# ip 80.30.30.33/24
OS900(config-vif4)# name Lupo4
OS900(config-vif4)# exit

OS900(config)# spanning-tree
OS900(config-mstp)# instance 1 priority 8192
accepted: dec=4096 or hex=0x1000
OS900(config-mstp)# instance 2 priority 4096
accepted: dec=8192 or hex=0x2000
OS900(config-mstp)# instance 1 port 1-3 priority 16
OS900(config-mstp)# instance 1 port 4 priority 32
OS900(config-mstp)# instance 1 port 1-4 path-cost auto
OS900(config-mstp)# instance 2 port 1-4 path-cost auto
OS900(config-mstp)# enable
OS900(config-mstp)#
```

# Viewing Spanning-Tree State

To display information on the ports participating in a specific MSTI, invoke the command:

**`show spanning-tree instance <0-64>`**

where,

**`<0-64>`**: Range of valid MSTI IDs from which one ID is to be selected.

Example

```
OS900(config-mstp)# show spanning-tree instance 1

Instance:          id=1 name='MSTi1'
Ports:
Tags:              999
BridgeId:          1001-000fbd0005b2  Bridge Priority:      4096 (0x1000)
Designated Root:   1001-000fbd0005b2
Root Port:         none (RootBridge)
Designated Brdg:   1001-000fbd0005b2
remainingHops:     14                 Instance MaxHops:     14
Topology Change Count:                0
Time Since Topology Change:           00:06:28
OS900(config-mstp)#
```

# Viewing Port States

To display information on the ports participating in a specific MSTI, invoke the command:

**`show instance <0-64> [ports PORTS-GROUP]`**

where,

**`<0-64>`**: Range of valid MSTI IDs from which one ID is to be selected.

**`Ports`**: Keyword which must be typed in if information is to be displayed on selective ports participating in the specific MSTI.

**`PORTS-GROUP`**: Group of ports participating in the specific MSTI.

Example

```
OS900(config-mstp)# show instance 1 port 3

Instance:    1     Tags: 110,120
Stp Port:  3     PortId: 1003 in 'MSTi1'
Priority:  16                       Uptime: 00:30:45
State:     Disabled
Int. PortPathCost: admin: Auto        oper: 20000000
Point2Point:       admin: ForceYes    oper: Yes
Partner:                              oper: MSTP
Edge:              admin: N      auto oper: N
MSTI msgs:         rx:   0            tx:   0

OS900(config-mstp)#
```

# BPDUs

## Policing

To drop BPDUs or flood their VLANs with them, invoke the command:

**`port PORTS-GROUP tagged-bpdu rx TAG-LIST (drop|flood)`**

where,

**`PORTS-GROUP`**: Group of Ports.

**`tagged-bpdu`**: Spanning Tree tagged-BPDU ports definition.

**`rx`**: For *recieved* BPDUs.

**`TAG-LIST`**: Tags of BPDUs to be dropped/flooded.

**`drop`**: Drop the BPDUs.

**`flood`**: Flood the BPDUs.

To revoke policing (dropping or tunneling subscriber's BPDUs), invoke the command:

**`no port PORTS-GROUP tagged-bpdu rx TAG-LIST (drop|flood)`**

## Tagging

For interoperability it is sometimes necessary to accept and transmit BPDUs after tagging them. To tag and transmit BPDUs, invoke the command:

**`port PORTS-GROUP tagged-bpdu tx TAG`**

where,

**`PORTS-GROUP`**: Group of Ports.

**`tagged-bpdu`**: Spanning Tree tagged-BPDU ports definition.

**`tx`**: For BPDUs to be *transmitted*.

**`TAG`**: Tag for transmitted BPDUs.

By default, the tagged BPDUs will be received and treated as untagged BPDUs so that they are transmitted rather than dropped.

To revoke tagging of BPDUs, invoke the command:

**`no port PORTS-GROUP tagged-bpdu tx TAG`**

# IEEE 802.1ag Port Forwarding

In some scenarios, spanning-tree port forwarding decisions based on IEEE 802.1ag will reduce convergence (recovery) time.

## Enabling

To enable port forwarding decisions based on IEEE 802.1ag:

1. From **`configure terminal`** mode, enter **`spanning-tree`** mode.
2. Invoke the command:
   **`port PORTS-GROUP oam-based-force-edge`**
   where,
   **`PORTS-GROUP`**: Group of ports to be enabled to forward based on IEEE 802.1ag decisions.

## Disabling

To disable port forwarding decisions based on IEEE 802.1ag:

1. From **`configure terminal`** mode, enter **`spanning-tree`** mode.
2. Invoke the command:
   **`no port PORTS-GROUP oam-based-force-edge`**
   where,
   **`PORTS-GROUP`**: Group of ports to be disabled from forwarding based on IEEE 802.1ag decisions.

# Filtering Events

Events can be filtered per the IEEE 802.1ag standard as follows:

1. From **`configure terminal`** mode, enter **`spanning-tree`** mode.
2. Invoke the command:
   **`oam-filter all|NUMBER all|NUMBER all|NUMBER all|NUMBER`**
   where,
   **`all`**: (First Appearance) Accept events from *all domains*.
   **`NUMBER`**: (First Appearance) Accept events from *a specific domain*.
   **`all`**: (Second Appearance) Accept events from *all services*.
   **`NUMBER`**: (Second Appearance) Accept events from *a specific service*.
   **`all`**: (Third Appearance) Accept events from *all MEPs*.
   **`NUMBER`**: (Third Appearance) Accept events from *a specific MEP*.
   **`all`**: (Fourth Appearance) Accept events from *all RMEPs*.
   **`NUMBER`**: (Fourth Appearance) Accept events from *a specific RMEP*.

# Transmit-Hold Count

The Transmit-Hold Count parameter controls the number of BPDUs that can be sent before pausing for 1 second. Setting a higher value than that of the default can significantly impact CPU utilization. A lower value may slow down convergence (recovery).

## Changing

To change the Transmit-Hold Count parameter value:

1. From **`configure terminal`** mode, enter **`spanning-tree`** mode.
2. Invoke the command:
   **`tx-hold-count <1-10>|infinite`**
   where,

**<1-10>**: Range of transmit-hold counts. A number from this range designates the number of BPDUs that will be sent per 1-second pause. Default: **6**.

**infinite**: No pause for any number of BPDUs.

## Default

To set the Transmit-Hold Count parameter value to the default value (6 BPDUs per 1-second pause):

1. From **configure terminal** mode, enter **spanning-tree** mode.
2. Invoke the command:
   **no tx-hold-count**

# Port Recovery

To recover isolated ports (i.e., to allow them to reconnect to the network):

1. Enter **configure terminal** mode.
2. Invoke either of the following commands:
   **port PORTS-GROUP recover**
   **recover (PORTS-GROUP|all)**
   where,
   **PORTS-GROUP**: Group of ports to be recovered.
   **all**: All ports to be recovered.

Example

```
OS904(config-mstp)# recover 1,3
port 1 state set to 'ENABLE'
port 3 state set to 'ENABLE'
OS904(config-mstp)#
```

# Chapter 9: ITU-T G.8032/Y.1344 Ethernet Ring Protection Switching (ERPS)

## General

This chapter shows how to configure an OS900 to provide Ethernet-Ring Protection Switching that is compliant to *ITU-T Recommendation G.8032/Y.1344 (06/2008)*.

The advantages of ERPS protocol over the spanning-tree protocols are: An virtually unlimited number of nodes in a ring is supported and recovery time for rings with a large number of nodes is shorter.

The disadvantage of ERPS protocol in comparison to spanning-tree protocols is that it supports only ring topologies.

## Terms and Concepts

**ERPS:** Ethernet-Ring Protection Switching.

**ERPS Group**: The group of nodes through which the same VLAN-based traffic is to pass.

**Group ID**: The ID assigned to all nodes of an ERPS group.

**APS:** Automatic Protection Switching protocol as defined in the ITU-T G.870 recommendation.

**R-APS Messages:** Ring-APS protocol messages as defined in the Y.1731 and G.8032 standards.

**Primary VLAN**: VLAN used for trafficking R-APS messages.

**APS Channel:** Automatic Protection Switching ring-wide VLAN used exclusively for transmission of OAM messages, including R-APS messages.

**Signal Failure (SF):** R-APS declaration of failure (as defined in the Y.1731 and G.8032 standards).

**RPL Owner:** Node that prevents traffic flow on one of its links in the ring during Idle State (in order to prevent logical looping of the ring) and allows traffic flow on the link in the Protection State. It does this by blocking and unblocking its port connected to the link. The link is referred to as Ring Protection Link (RPL).

**RPL Port:** Port of RPL Owner connected to the RPL.

**Ring Port:** Port of a node in a ring that is to transmit and receive R-APS messages.

**Access Port:** Port of a node in a ring that is not to be connected in the ring but which transmits/receives non-APS traffic to/from the ring.

**Idle State:** Normal state of ring nodes (e.g., OS900s), i.e., RPL port blocked and all nodes and ports operational.

**Protection State:** ERPS mechanism active due to Local SF or R-APS (SF). RPL port is unblocked while ports of faulty links are blocked.

**Link Monitoring:** Use of Y.1731 Ethernet Continuity Check Messages (CCMs) to check the integrity of inter-node links in the ring.

**No Request (NR):** R-APS declaration that there are no failure conditions (e.g., SF, etc.) on the node. In particular, NR is sent by the two nodes on a failed link when the link recovers.

**Guard Timer:** Guard Timer causes the node whose port has recovered to ignore R-APS messages for a preset time period.

**WTR Timer:** Wait-To-Restore Timer causes the RPL Owner to wait for a preset time period before attempting to set the network in the Idle State when the RPL Owner receives an NR from the node whose port has recovered. WTR is used exclusively by the RPL Owner.

**HO Timer:** Hold-Off Timer disables the ERPS mechanism for a time period in order to allow intermittent link transients to die out or to allow some other agent, operating at a lower layer than the ERPS mechanism, to stabilize the ring.

**Major-Ring**: The Ethernet Ring in a Multi-Ring Ladder topology that controls the link shared with all the other rings (called Sub-Rings).

**Sub-Ring**: An Ethernet Ring in a Multi-Ring Ladder topology that is connected to the Major-Ring through the use of interconnection nodes. On their own, the Sub-Ring links do not form a closed physical loop. A closed loop may be formed by the Sub-Ring links and the link between interconnection nodes that is controlled by the Major-Ring.

**Virtual Channel**: The R-APS channel connection between two interconnection nodes of a Sub-Ring over a network or other ring. Its connection characteristics (e.g., path, performance, etc.) are influenced by the characteristics of the network (e.g., ring) providing connectivity between the interconnection nodes.

**Virtual Port**: Either of the two ports at the ends of the link carrying the Virtual Channel.

**Channel Blocking**: A mode of operation in which traffic blocking is VLAN-tag based.

**Load Balancing**: In a Single-Ring topology network, traffic from a node is divided on the basis of VLAN tag and sent in opposite directions (clockwise, counterclockwise) along the two arms of the ring.

# Definition

ERPS is a mechanism that uses the APS protocol and complies with the ITU-T SG15/Q9 G.8032 standard for providing operation protection to Ethernet networks having a physical ring topology when a link fails.

# Scope

The ERPS mechanism provides protection if only one link fails. If more links fail it indicates such failure.

A ring network can be built of switches, only some of which will run the ERPS mechanism, and still make protection effective. For such networks, each link must have at least one switch that runs ERPS connected to it. If a link does not have at least one switch that runs ERPS, ring protection can be provided by connecting these two switches to ERPS-capable switches and running the IEEE 802.1ag and ITU-T SG 13 Y.1731 standard Ethernet OAM protocol between the ERPS-capable switches – see *Figure 29*, page *232*.

ERPS in the OS900 supports the following physical network topologies:

- Single Ring
- Multi-Ring Ladder

Traffic load balancing can be configured on Single-Ring topology networks.

# Ring States

The ring network can be in either one of the following states:

- Idle State
- Protection State

## Idle State

In Idle State:

- All nodes of the physical network are connected in ring topology
- ERPS prevents loops in the network by blocking the RPL port
- Optionally, Link Monitoring may be performed for every link by both nodes on the link

## Protection State

In Protection State:

- Nodes detect Local SF and blocked failed ports, and report this failure by sending an R-APS (SF) message periodically

– On receiving R-APS (SF), RPL Owner unblocks the RPL port, and all nodes perform Learn Table flushing

# Failure Recovery

The following actions are performed during failure recovery at the end of which the ring network returns to Idle State:

– When a node detects Clear SF, it continually sends R-APS (NR) and keeps the failed port blocked
– The RPL Owner receives R-APS (NR) from the nodes on the recovered link and starts the WTR timer
– When the time set on the WTR expires, RPL Owner blocks the RPL port, flushes its Learn Table, and transmits R-APS (NR, RB) message
– When the nodes receive the R-APS (NR, RB) message they flush their Learn Table and unblock their blocked ports to allow data traffic to flow through them

# Principle of Operation

When ERPS is activated, the nodes in the ring undergo ERPS initialization. During initialization, all ports remain blocked to data traffic and each node sends R-APS (NR) and checks the state of the two links connected to its ports.

Case 1 – All links Up: If all links are up, the nodes send an R-APS (NR) to the RPL Owner. If the node is an RPL Owner it unblocks the port that is not connected to the RPL and instructs all the other nodes, using R-APS (NR, RB) message, to unblock their ports for data traffic flow. As a result, the network enters Idle State.

Case 2 – A link is Down: If a link other than the RPL is down, the two nodes that are connected at either end of the failed link block their ports to data traffic flow and send an R-APS (SF) to the RPL Owner via the APS channel. When the RPL Owner receives R-APS (SF) it unblocks its RPL port (so that the RPL can be used for data traffic flow) and flushes its Learn Table. The other nodes, on receiving R-APS (SF), flush their Learn Table. As a result, the network enters Protection State.

When the failed port recovers, the failure recovery process (as described in the section *Failure Recovery*, page *227*) is started.

If load balancing is activated in a Single-Ring topology, traffic from a node is divided on the basis of VLAN tag and sent in opposite directions along the two arms of the ring.

# Rules

1. All nodes in the same ring that are to run the same ERPS group must be assigned the same Group ID.
2. One and only one node in a ring that is capable of running ERPS must be configured as an RPL Owner.
3. The Ring Ports and the Access Ports can be included in the same VLAN.
4. Ring Ports and Access Ports may be trunks. (Trunking is described in ***Chapter 13:*** *IEEE 802.3ad Link Aggregation (LACP)*, page *273*.)

# Single Ring

## Configuration

### Procedure

The procedure given below applies when all switches in the ring are ERPS-capable.

For a ring in which not all switches are ERPS-capable, Example 2 (below) can serve to demonstrate how each switch is to be configured in order to provide ERPS.

RPL Owner

1. Make sure that the ring is physically open.
2. Enter `configure terminal` mode.

3. Optionally, set the ports in tag outbound mode using the command **`port tag-outbound-mode tagged PORTS-GROUP`**.
4. Create an Inband VLAN Interface that includes all the Ring Ports and the Access Ports.
5. Assign a Group ID to the node using the command:

   **`erp <0-7>`**

   where,

   **`<0-7>`**: Range of Group IDs from which one is to be selected.

   (To delete the Group ID, invoke the command **`no erp <0-7>`**.)
6. Confer RPL Ownership using the command:

   **`rpl-owner`**

   (To revoke the setting of the node as an RPL Owner, invoke the command **`no rpl-owner`**.)
7. Select one of the two Ring Ports of the RPL Owner to be blocked using either one of the following commands:

   **`rpl-port west-port`**

   Or

   **`rpl-port east-port`**

   (To revoke either of the above commands, invoke the command **`no rpl-port (west-port|east-port)`**.)
8. Specify the West port (*Figure 28* and *Figure 29* show West ports as 2) using the command:

   **`west-port PORT`**

   where,

   **`PORT`**: Number of the West port

   (To revoke the setting of the port as West port, invoke the command **`no west-port PORT`**.)
9. Specify the East port (*Figure 28* and *Figure 29* show East ports as 1) using the command:

   **`east-port PORT`**

   where,

   **`PORT`**: Number of the East port

   (To revoke the setting of the port as East port, invoke the command **`no east-port PORT`**.)
10. Set up an APS channel in the Inband VLAN Interface created in Step *4* above using the command:

    **`primary-vlan <1-4095>`**

    where,

    **`<1-4095>`**: Tag (VID) of Inband VLAN Interface that includes the Ring Ports.

    (To delete the APS channel, invoke the command **`no primary-vlan`**.)
11. Activate ERPS by invoking the command:

    **`enable`**

    (To deactivate ERPS, invoke the command **`no enable`**.)
12. Close the ring physically.

<u>Non-RPL Owner</u>

1. Enter **`configure terminal`** mode.
2. Optionally, set the ports in tag outbound mode using the command **`port tag-outbound-mode tagged PORTS-GROUP`**.
3. Create an Inband VLAN Interface that includes all the Ring Ports and the Access Ports and whose tag is the same as that used in Step *4* above.
4. Assign a Group ID to the node with a value that is the same as that used in Step *5* above using the command:

   **`erp <0-7>`**

   where,

**<0-7>**: Range of Group IDs from which one is to be selected.

(To delete the Group ID, invoke the command **no erp <0-7>**.)

5. Specify the West port (*Figure 28* and *Figure 29* show West ports as 2) using the command:

**west-port PORT**

where,

**PORT**: Number of the West port

(To revoke the setting of the port as West port, invoke the command **no west-port PORT**.)

6. Specify the East port (*Figure 28* and *Figure 29* show East ports as 1) using the command:

**east-port PORT**

where,

**PORT**: Number of the East port

(To revoke the setting of the port as East port, invoke the command **no east-port PORT**.)

7. Set up an APS channel in the Inband VLAN Interface created in Step *3* above using the command:

**primary-vlan <1-4095>**

where,

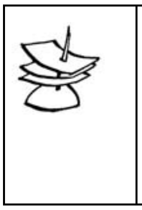
**<1-4095>**: Tag (VID) of Inband VLAN Interface that includes the Ring Ports.

(To delete the APS channel, invoke the command **no primary-vlan**.)

8. Activate ERPS by invoking the command:

**enable**

(To deactivate ERPS, invoke the command **no enable**.)



**Note**

If it is required to change any of the configuration settings in the procedure after the command **enable** has been executed, first invoke the command **no enable**.

If the command **no enable** is performed on the RPL Owner, its two Ring Ports are unblocked which may form a loop in the network!

**Example 1**

The purpose of this example is to show how switches (interconnected in a physical ring) are to be configured so that the ring's operation can be protected. All switches in the ring are ERPS-capable. This gives the ring *full* protection. For clarity, only four nodes are used. East ports are numbered 1. West ports are numbered 2.

***Network***

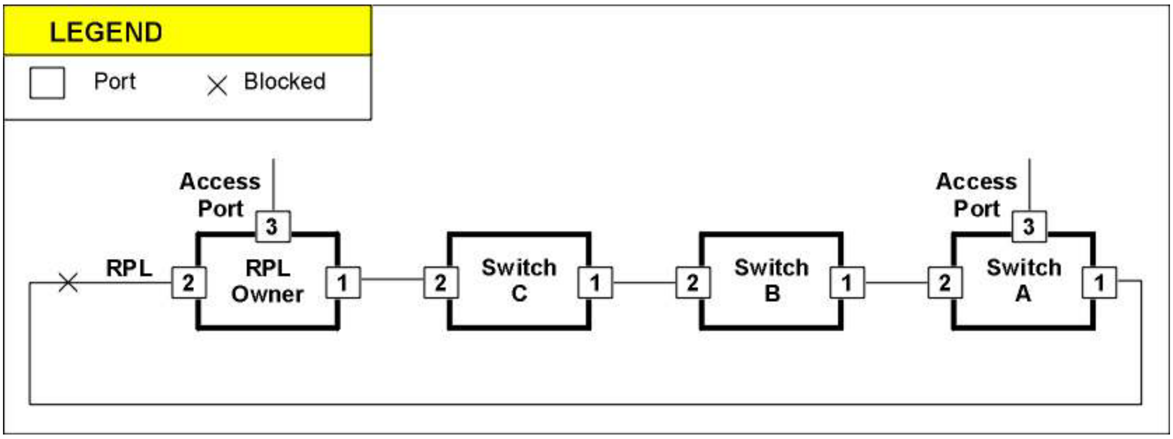



**Figure 28: Standard Ring Network (All Nodes Running ERPS)**

***Implementation***

**Standard Ring**

**RPL Owner**

----------Disabling the RPL Port----------

```
port state disable 2
```

----------Enabling multi-VLAN membership (Optional)----------

```
port tag-outbound-mode tagged 1-3
!
```

----------Creating Inband VLAN Interface for the two Ring Ports and Access Port----------

```
interface vlan vif10
 tag 10
 ports 1-3
!
```

----------Assigning Group ID----------

```
erp 1
```

----------Conferring RPL Ownership----------

```
 rpl-owner
```

----------Selecting West Port of RPL Owner to be blocked----------

```
 rpl-port west-port
```

----------Specifying the West Port of RPL Owner----------

```
 west-port 2
```

----------Specifying the East Port of RPL Owner----------

```
 east-port 1
```

----------Setting up an APS Channel----------

```
 primary-vlan 10
```

----------Activating ERPS----------

```
 enable
!
```

----------Enabling the RPL Port----------

```
 port state enable 2
```

**Switch A**

-----------------------------------------Enabling multi-VLAN membership (Optional)-----------------------------------------

```
port tag-outbound-mode tagged 1-3
!
```

----------------------Creating Inband VLAN Interface for the two Ring Ports and Access Port----------------------

```
interface vlan vif10
 tag 10
 ports 1-3
!
```

----------------------------------------------------------Assigning Group ID----------------------------------------------------------

```
erp 1
```

------------------------------------------------------Specifying the West Port------------------------------------------------------

```
 west-port 2
```

------------------------------------------------------Specifying the East Port------------------------------------------------------

```
 east-port 1
```

---------------------------------------------------Setting up an APS Channel---------------------------------------------------

```
 primary-vlan 10
```

-----------------------------------------------------------Activating ERPS-----------------------------------------------------------

```
enable
!
```

**Switch B**

--------------------------------Same as for **Switch A** except that Port 3 is to be excluded--------------------------------
(because of the way its ports are connected in the network)

**Switch C**

--------------------------------------------------------Same as for **Switch B**--------------------------------------------------------
(because of the way its ports are connected in the network)

### Example 2

The purpose of this example is to show how switches (interconnected in a physical ring) are to be configured so that the ring's operation can be protected. Only two switches in the ring are ERPS-capable. The two non-ERPS-capable switches have a common link. If this link fails ERPS cannot perform network operation recovery. If any other link fails, ERPS can. This means that ERPS gives the ring only *partial* protection. Running Ethernet Service OAM in addition to the ERPS protocol can provide full protection. ***Chapter 21:*** *IEEE 802.1ag and ITU-T Y.1731 Ethernet Service OAM*, page *385* details Ethernet Service OAM. CCMs are run between East Port **1** and West Port **2**.

East ports are numbered 1. West ports are numbered 2.

***Network***

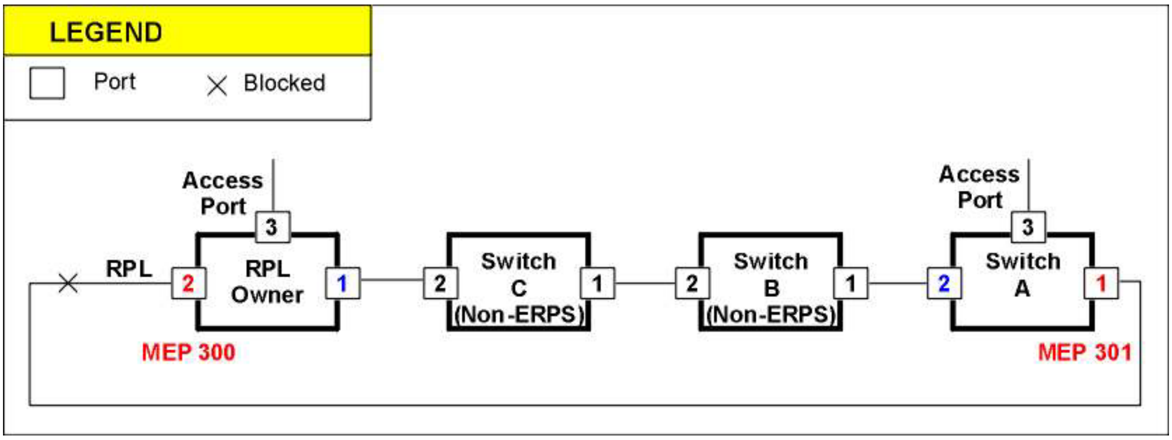



**Figure 29: Non-Standard Ring Network (Only some Nodes Running ERPS)**

***Implementation***

**Non-Standard Ring**

**RPL Owner**

------------------------------------------Enabling multi-VLAN membership (Optional------------------------------------------

```
port tag-outbound-mode tagged 1-3
!
```

-----------------------Creating Inband VLAN Interface for the two Ring Ports and Access Port-----------------------

```
interface vlan vif10
 tag 10
 ports 1-3
!
```

---------------------------------------------------------Assigning Group ID---------------------------------------------------------

```
erp 1
```

----------------------------------------------------Conferring RPL Ownership----------------------------------------------------

```
 rpl-owner
```

---------------------------------------------------Setting up an APS Channel---------------------------------------------------

```
 primary-vlan 10
```

-----------------------------------Selecting West Port of RPL Owner to be blocked-----------------------------------

```
 rpl-port west-port
```

-------------------------------------------Specifying the West Port of RPL Owner-------------------------------------------

```
 west-port 2
```

-------------------------------------------Specifying the East Port of RPL Owner-------------------------------------------

```
 east-port 1
```

-----------------------Unblocking Port **1** if RPL Owner does not receive CCM from MEP **301**-----------------------
(Optional)

```
 activate-ccm domain 4 service 7 rmep 301 east-port
```

-------------------------------------------------------Activating ERPS-------------------------------------------------------

```
 enable
!
```

---------------------------------------------Creating an Ethernet OAM *domain*---------------------------------------------

```
ethernet oam domain 4
```

-----------------------------------Creating a *service* in the Ethernet OAM domain-----------------------------------

```
  service 7
```

----Specifying the VLAN to participate in the service as that containing the Ring and Access Ports----

```
    vlans 10
```

-----------------------Specifying the remote MEPs that are to participate in the service-----------------------

```
    remote-meps 301
```

-------------------------Specifying the port via which MEP 300 is *not* to send CCMs--------------------------

```
    mep 300 port 2
```

-------------------------------------------------------Activating MEP 300-------------------------------------------------------

```
    mep 300 activate
```

-----------------------------------------Preventing MEP 300 from sending TLV-----------------------------------------
(Optional)

```
    no mep 300 send-port-tlv
    no mep 300 send-interface-tlv
```

---------------------------Enabling MEP 300 to send CCMs (when Ethernet OAM is enabled----------------------

```
    mep 300 ccm-activate
!
```

-------------------------------------------------Enabling Ethernet OAM-------------------------------------------------

```
ethernet oam enable
```

**Switch A**

-----------------------------------------Enabling multi-VLAN membership (Optional)-----------------------------------------

```
port tag-outbound-mode tagged 1-3
!
```

----------------------Creating Inband VLAN Interface for the two Ring Ports and Access Port----------------------

```
interface vlan vif10
 tag 10
 ports 1-3
!
```

----------------------Creating Inband VLAN Interface for the two Ring Ports and APS Channel----------------------

```
interface vlan vif20
 tag 20
 ports 1-2
!
```

--------------------------------------------------------Assigning Group ID--------------------------------------------------------

```
erp 1
```

-------------------------------------------------Setting up an APS Channel-------------------------------------------------

```
 primary-vlan 20
```

------------------------------------------Specifying the West Port of RPL Owner------------------------------------------

```
 west-port 2
```

------------------------------------------Specifying the East Port of RPL Owner------------------------------------------

```
 east-port 1
```

------------------------Unblocking Port **2** if RPL Owner does not receive CCM from MEP **300**------------------------

```
 activate-ccm domain 4 service 7 rmep 300 west-port
```

----------------------------------------------------Activating ERPS----------------------------------------------------

```
 enable
!
```

-------------------------------------------Creating an Ethernet OAM *domain*-------------------------------------------

```
ethernet oam domain 4
```

----------------------------------Creating a *service* in the Ethernet OAM domain----------------------------------

```
  service 7
```

---Specifying the VLAN to participate in the service as that containing the Ring and Access Ports---

```
    vlans 10
```

-----------------------Specifing the remote MEPs that are to participate in the service-----------------------

```
    remote-meps 300
```

---------------------------Specifing the port via which MEP 301 is *not* to send CCMs---------------------------

```
    mep 301 port 1
```

-------------------------------------------------------Activating MEP 301-------------------------------------------------------

```
    mep 301 activate
```

-----------------------------------------Preventing MEP 301 from sending TLV-----------------------------------------
(Optional)

```
    no mep 301 send-port-tlv
    no mep 301 send-interface-tlv
```

---------------------Enabling MEP 301 to send CCMs (when Ethernet OAM is enabled)---------------------

```
    mep 301 ccm-activate
!
```

-----------------------------------------------------Enabling Ethernet OAM-----------------------------------------------------

```
ethernet oam enable
```

**Switch B (Non-ERPS)**

---------------------------------------Enabling multi-VLAN membership (Optional) ---------------------------------------

```
port tag-outbound-mode tagged 1-3
!
```

-----------------------Creating Inband VLAN Interface for the two Ring Ports and Access Port-----------------------

```
interface vlan vif10
 tag 10
 ports 1-3
!
```

**Switch C (Non-ERPS)**

-----------------------------------------------------Same as for **Switch B**-----------------------------------------------------
(because of the way its ports are connected in the network)

**Example 3**

The purpose of this example is to show how OS900s are to be configured in a Single Ring network to provide traffic load balancing using the ERPS protocol.

Specifically, egress traffic from a node is divided on the basis of VLAN tag and sent in opposite directions (clockwise, counterclockwise) along the two arms of the ring as long as the ring is in the stable (idle) state. If a link on either arm goes down, the traffic that was to go through the faulty link will be directed to go through the other arm.

To provide load balancing, two ERPS Groups must be created. For one ERPS Group, traffic belonging to one group of VLANs will be blocked at a Ring Port (called, say, East) of the node. For the ERPS Group, traffic belonging to the other group of VLANs will be blocked at another Ring Port (called, say, West) of the same node.

In order to divide the traffic load between the two arms of the ring, two ERPS Groups must be created. As a result, two RPL Owners are required (one per ERPS Group), one for the West Port and the other for the East Port.

In this example we will configure two ERPS Groups, one for each group of VLANs, and we'll ensure that two groups can flow only in opposite directions on the ring. Also, one RPL Owner will be defined for the two ERPS Groups.

***Network***

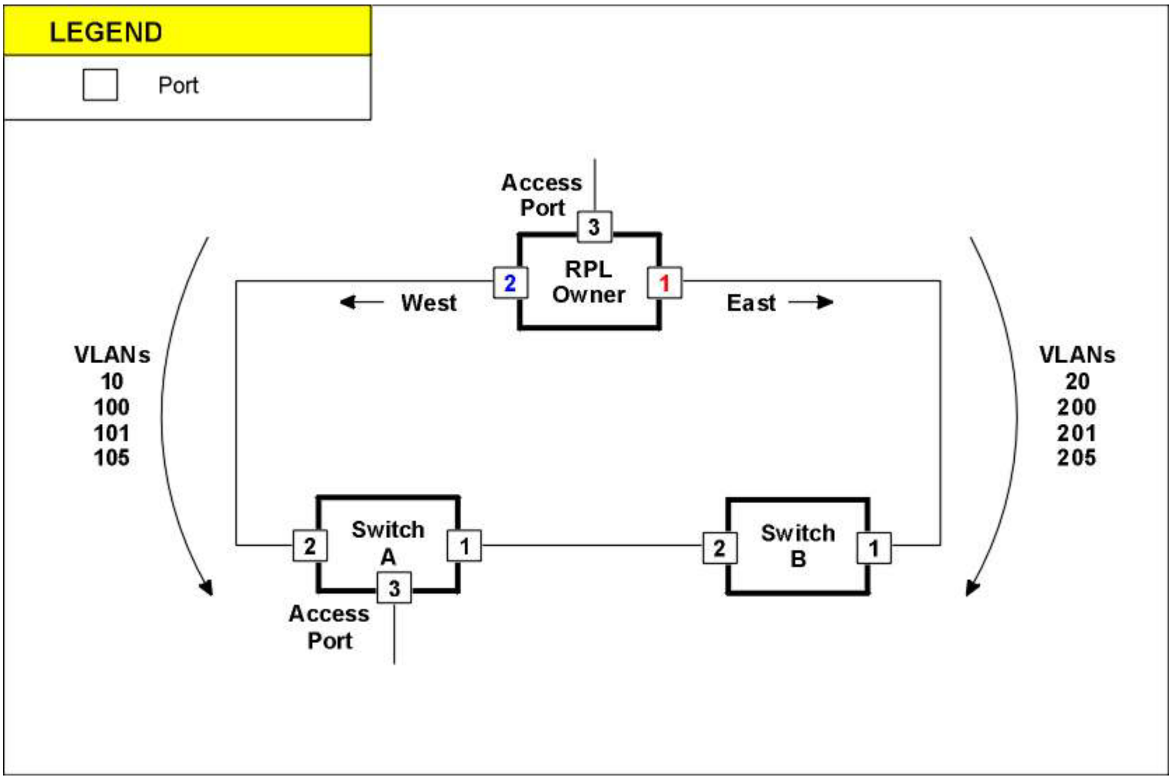



**Figure 30: Standard Ring Network with Traffic Load Balancing**

***Implementation***

**Standard Ring with Traffic Load Balancing**

**RPL Owner**

--------------------------------------------------Enabling multi-VLAN Membership-----------------------------------------------

```
port tag-outbound-mode tagged 1-3
!
```

---Creating Inband VLAN Interfaces for the Two Ring Ports and Access Port to be used on multiple VLANs---

```
interface vlan vif10
 tag 10
 ports 1-3
!
interface vlan vif100
 tag 100
 ports 1-3
```

```
!
interface vlan vif101
 tag 101
 ports 1-3
!
interface vlan vif105
 tag 105
 ports 1-3
!
interface vlan vif20
 tag 20
 ports 1-3
!
interface vlan vif200
 tag 200
 ports 1-3
!
interface vlan vif201
 tag 201
 ports 1-3
!
interface vlan vif205
 tag 205
 ports 1-3
!

------------------------------Assigning Group ID------------------------------

erp 1

------------------------------Conferring RPL Ownership------------------------------

 rpl-owner

------------------------------Selecting West Port of RPL Owner to be Blocked------------------------------

 rpl-port east-port

------------------------------Setting up the APS Channel------------------------------

 primary-vlan 10

------------------------------Assigning the VLANs to be Associated with the First ERPS Group------------------------------

 vlans 10,100,101,105

------------------------------Specifying the West Port of RPL Owner------------------------------

 west-port 2

------------------------------Specifying the East Port of RPL Owner------------------------------

 east-port 1

------------------------------Configuring the ERPS Group to Operate in Channel Blocking Mode------------------------------

 channel-blocking

------------------------------Activating ERPS------------------------------
```

```
 enable
!
```

---------------------------------------------------Assigning New Group ID for other VLANs----------------------------------

```
erp 2
```

---------------------------------------------------Conferring RPL Ownership---------------------------------------------------

```
 rpl-owner
```

----------------------------------Selecting East Port of RPL Owner to be blocked----------------------------------

```
 rpl-port west-port
```

------------------------------------------------Setting up the APS Channel--------------------------------------------------

```
 primary-vlan 20
```

--------------------Assigning the VLANs to be associated with the Second ERPS Group--------------------

```
 vlans 20,200,201,205
```

-----------------------------------------Specifying the West Port of RPL Owner------------------------------------------

```
 west-port 2
```

------------------------------------------Specifying the East Port of RPL Owner-------------------------------------------

```
 east-port 1
```

--------------------------Configuring the ERPS Group to Operate in Channel Blocking Mode--------------------------

```
 channel-blocking
```

-----------------------------------------------------------Activating ERPS-------------------------------------------------------

```
 enable
!
```

**Switch A**

-----------------------------------------------Enabling multi-VLAN Membership -----------------------------------------------

```
port tag-outbound-mode tagged 1-3
!
```

----------------------Creating Inband VLAN Interfaces for the two Ring Ports and Access Port----------------------

```
interface vlan vif10
 tag 10
 ports 1-3
!
interface vlan vif100
 tag 100
 ports 1-3
!
interface vlan vif101
```

```
 tag 101
 ports 1-3
!
interface vlan vif105
 tag 105
 ports 1-3
!
interface vlan vif20
 tag 20
 ports 1-3
!
interface vlan vif200
 tag 200
 ports 1-3
!
interface vlan vif201
 tag 201
 ports 1-3
!
interface vlan vif205
 tag 205
 ports 1-3
!

------------------------------------------------------------Assigning Group ID------------------------------------------------------------

erp 1


----------------------------------------------------Setting up the APS Channel----------------------------------------------------

 primary-vlan 10

----------------------Assigning the VLANs to be Associated with the First ERPS Group----------------------

 vlans 10,100,101,105

---------------------------------------------Specifying the West Port of RPL Owner---------------------------------------------

 west-port 2

---------------------------------------------Specifying the East Port of RPL Owner--------------------------------------------

 east-port 1

---------------------------Configuring the ERPS Group to Operate in Channel Blocking Mode---------------------------

 channel-blocking

-----------------------------------------------------------Activating ERPS-----------------------------------------------------------

 enable
!
----------------------------------------------------- Assigning New Group ID for other VLANs----------------------------------

erp 2

---------------------------------------------------Setting up the APS Channel---------------------------------------------------
```

```
 primary-vlan 20
```

-------------------Assigning the VLANs to be Associated with the Second ERPS Group-------------------

```
 vlans 20,200,201,205
```

-----------------------------------------Specifying the West Port of RPL Owner------------------------------------------

```
 west-port 2
```

------------------------------------------Specifying the East Port of RPL Owner------------------------------------------

```
 east-port 1
```

---------------------------Configuring the ERPS Group to Operate in Channel Blocking Mode---------------------------

```
 channel-blocking
```

----------------------------------------------------------Activating ERPS----------------------------------------------------------

```
 enable
!
```

**Switch B**

--------------------------------Same as for **Switch A** except that Port 3 is to be excluded--------------------------------
(because of the way its ports are connected in the network)

# Multi-Ring Ladder

## General

A Sub-Ring is a ring in the multi-ring ladder network which shares a link with the Major-Ring but, for the use of the ERPS protocol, it is assumed to be without the shared link. By itself, the Sub-Ring does not create a closed loop. The Sub-Ring is connected to the Major-Ring or network through the use of Interconnection Nodes.

The Virtual Channel is the R-APS channel created between the two Interconnection Nodes of a Sub-Ring. In other words, it is the channel created between the two interconnected ports on the shared link.

To explain the need for these two concepts, we use *Figure 31*, page *242*. Suppose we define rings A, B, G, H and B, C, F, G as regular ERPS rings with a shared links. In these rings, we can define two ERPS Groups in which nodes A and C can be RPL Owners and ports A1 and C2 as RPL Ports. In a stable state, the network would face no major issues and no traffic loops would occur. However, if the shared link (B, G) fails, then both RPL Owners receive an R-APS (SF) signal and will unblock the RPL port. In this new situation, we would have a network loop.

To overcome this situation, we need to set one of the rings in the topology as a Sub-Ring, i.e. a ring that is not fully influenced by the status of the shared link and in which the originally blocked port would remain blocked even if the shared link fails.

To configure a Sub-Ring, simply define a Virtual Channel in the Sub-Ring. This is done by defining the node ports on the shared link as Virtual Channel ports. In *Figure 31*, page *242*, the Virtual channel is defined between ports B1 and G2.

As in Amendment 1, if the Shared Link (in the Major-Ring) fails, the Sub-Rings are not affected.

**Note**

A Virtual Channel is required for two or more rings only if the ports of the nodes are in the same VLAN.

## Example

In the example below, only the configuration of node B, which has one of its port connected to the virtual channel, is given. Configuration of the node G is similar, and configuration of the remaining nodes is similar to that of a Single Ring network. Four Inband VLAN Interfaces are created: with Tags 10, 20, 30 and 40 on the Major-Ring, Tags 20 and 40 on Sub-Ring 1 and Tags 30 and 40 on Sub-Ring 1. Accordingly, with reference to *Figure 31*, page *242*, a node, the associated Inband VLAN Interfaces, and member ports of the interface are as follows:

| Node | Interface | Ports | Node | Interface | Ports |
|---|---|---|---|---|---|
| A | 10 | 1-3 | E | 10 | – |
| | 20 | 1-3 | | 20 | – |
| | 30 | 1-3 | | 30 | 2-4 |
| | 40 | 1-3 | | 40 | 2-4 |
| B | 10 | 1,2 | F | 10 | – |
| | 20 | 1-3 | | 20 | 1-3 |
| | 30 | 1,2,4 | | 30 | – |
| | 40 | 1-4 | | 40 | 1-3 |
| C | 10 | – | G | 10 | 1,2 |
| | 20 | 1-3 | | 20 | 1-3 |
| | 30 | – | | 30 | 1,2,4 |
| | 40 | 1-3 | | 40 | 1-4 |
| D | 10 | – | H | 10 | 1-3 |
| | 20 | – | | 20 | 1-3 |
| | 30 | 2-4 | | 30 | 1-3 |
| | 40 | 2-4 | | 40 | 1-3 |

### Network

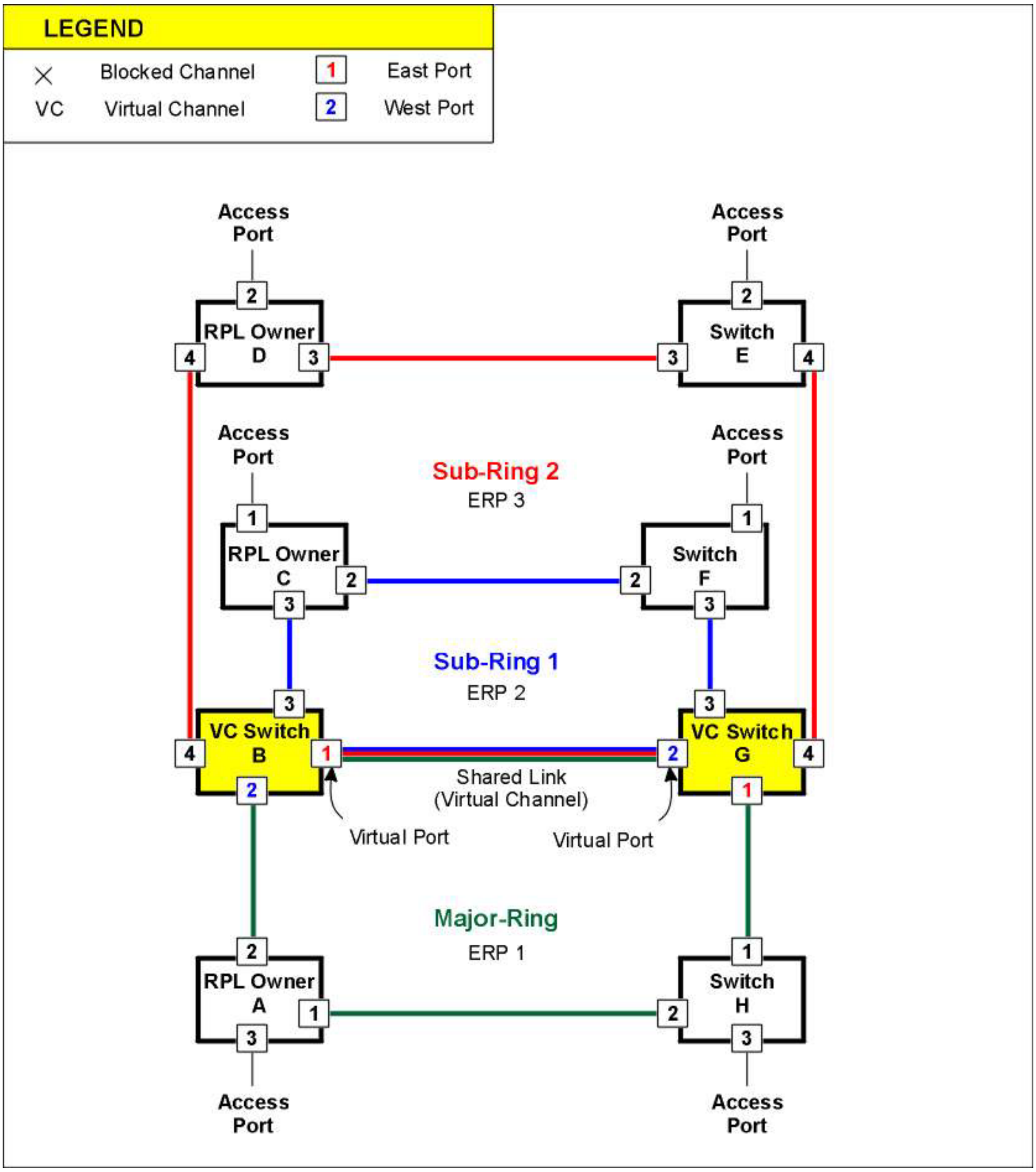



**Figure 31: Multi-Ring Ladder Network**

### Implementation

**Multi-Ring Ladder**

**VC Switch B**

------------------------------------------------Enabling multi-VLAN membership------------------------------------------------

```
port tag-outbound-mode tagged 1-4
!
```

--Creating Inband VLAN Interfaces for the two Ring Ports and Access Port to be Included in multiple VLANs--

```
interface vlan vif10
 tag 10
 ports 1,2

interface vlan vif20
 tag 20
 ports 1-3

interface vlan vif30
 tag 30
 ports 1,2,4

interface vlan vif40
 tag 40
 ports 1-4
!
------------------------------Assigning ERPS Group ID – this is the First Sub-Ring------------------------------

erp 1

---------------------------------------------Setting up the APS Channel---------------------------------------------------

 primary-vlan 10

-------------------------------------------Specifying the West Port of RPL Owner------------------------------------------

 west-port 3

-------------------------------------------Specifying the East Port of RPL Owner-----------------------------------------

 east-port 1

 enable
!

--------------------------Assigning ERPS Group ID – this is the Second Sub-Ring--------------------------

erp 2

-------------------------------------------------Setting up the APS Channel-------------------------------------------------

 primary-vlan 20

-----------------------------------------Specifying the West Port of RPL Owner----------------------------------------

 west-port 4

------------------------------ Specifying the East Port as a Part of the Virtual Channel------------------------------

 east-port 1 virtual-channel

 enable
!

-------------------------------ERPS Group ID – this is the Major-Ring-------------------------------
erp 3

-------------------------------------------------Setting up the APS Channel--------------------------------------------------
```

```
 primary-vlan 30
```

-------------------------------------Specifying the West Port of RPL Owner-------------------------------------------

```
 west-port 2
```

-------------------------------Specifying the East Port as a part of the virtual channel-------------------------------

```
 east-port 1 virtual-channel

 enable
!
```

**VC Switch G**

--------------------------------Similar to that of **VC Switch B** in this implementation) --------------------------------
(because of the way its ports are connected in the network)

**RPL Owners A, C, D, E, F, and H**

--------------Similar to **VC Switch B** but **RPL Owners** as in Standard Ring (see **Example 1**) --------------
(because of the way its ports are connected in the network)

# Optional Configuration Parameters

## Guard Timer

### Setting

By default, the Guard Timer is set for 500 ms.
To set the Guard Timer for a different period:

1. Enter the mode of the Group ID of the node by invoking the command:
   **`erp <0-7>`**
   where,
   `<0-7>`: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **`guard-timer <10-2000>`**
   where,
   `<10-2000>`: Wait time in milliseconds.

### Default

To set the Guard Timer to the default (`500` ms):

1. Enter the mode of the Group ID of the node by invoking the command:
   **`erp <0-7>`**
   where,
   `<0-7>`: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **`no guard-timer`**

## WTR Timer

Applies only for RPL Owner.

#### Setting

By default, the WTR Timer is set for 300 ms.

To set the WTR Timer for a different period:

1. Enter the mode of the Group ID of the node by invoking the command:
   **erp <0-7>**
   where,
   **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **wtr-timer <60-720>**
   where,
   **<60-720>**: Wait time in milliseconds. (Default = **300** ms).

#### Default

To set the WTR Timer to the default (**300** ms):

1. Enter the mode of the Group ID of the node by invoking the command:
   **erp <0-7>**
   where,
   **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **no wtr-timer**

### HO Timer

#### Setting

By default, the HO Timer is set for **0** second.

To set the HO Timer for a different period:

1. Enter the mode of the Group ID of the node by invoking the command:
   **erp <0-7>**
   where,
   **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **holdoff-timer <0-10>**
   where,
   **<0-10>**: Wait time in seconds. (Default = **0** s).

#### Default

To set the HO Timer to the default (**0** s):

1. Enter the mode of the Group ID of the node by invoking the command:
   **erp <0-7>**
   where,
   **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **no holdoff-timer**

## Viewing

### Defaults

To view ERPS default configuration information about the node:

1. Enter **enable** mode.
2. Invoke the command:
   **show erp defaults**

Example

```
OS904# show erp defaults
Parameter                        Default values
----------------------------------------------------------------
OAM:
  Destination MAC address         01-19-A7-00-00-01
  Ether-type                      8902
  RPL Owner                       no
  OAM CCM                         not activated
  enable                          no
Timers:
  Wait To Restore Timer           300 sec
  Guard Timer                     500 msec
  Holdoff Timer                   0 sec
OS904#
```

## Configuration

To view ERPS configuration information about the node:

1. Enter the mode of the Group ID of the node by invoking the command:
   **erp <0-7>**
   where,
   **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected
2. Invoke the command:
   **show configuration**

Example

```
OS904(config-erp-1)# show configuration
erp 1
 rpl-owner
 rpl-port west-port
 primary-vlan 20
 east-port 1
 west-port 2
 enable
OS904(config-erp-1)#
```

## Running Configuration

To view ERPS running configuration information about the node:

1. Enter **enable** mode.
2. Invoke the command:
   **show running-config erp**

Example

```
OS904# show running-config erp
erp 1
 rpl-owner
 rpl-port west-port
 primary-vlan 20
 east-port 1
 west-port 2
 enable
OS904#
```

## Configuration and Status

To view ERPS configuration and status information about the node:

1. Enter **enable** mode.
2. Invoke the command:

    **show erp <0-7>**

    where,

    **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected

Example

```
OS904# show erp 1
Group ID 1 is Enabled
=======================
RPL-Owner: Yes
RPL Port:  West port
Primary VLAN: 20
East port: 1, state SF
West port: 2, state SF
Timers details
--------------
  WTR interval:         300 [sec]
  Guard interval:       500 [msec]
  Holdoff interval:     0 [sec]
State Machine info
------------------
Event             Current State          Prev State
---------------------------------------------------
Local SF          Protecting           Init
OS904#
```

## Configuration, Status, and Statistics

To view ERPS configuration, status, and statistical information about the node:

1. Enter **enable** mode.
2. Invoke the command:

    **show erp <0-7> details**

    where,

    **<0-7>**: Range of Group IDs from which the Group ID of the node is to be selected

Example

```
OS904# show erp 1 details
Group ID 1 is Enabled
=======================
RPL-Owner: Yes
RPL Port:  West port
Primary VLAN: 20
East port: 1, state SF
West port: 2, state SF
Timers details
--------------
  WTR interval:         300 [sec]
  Guard interval:       500 [msec]
  Holdoff interval:     0 [sec]
State Machine info
------------------
Event              Current State          Prev State
---------------------------------------------------
Local SF           Protecting           Init
Raps statistics
---------------
  RAPS sent:                         0
  RAPS received:                     0
  Local SF happened:                 0
  Remote SF happened:                0
  Local Clear SF happened:           0
  NR event happened:                 0
  NR-RB event happened:              0
Timers status
-------------
  WTR timer is Running:                 No
  Guard timer is Running:               No
  Holdoff timer is Running:             No
  Raps timer is Running:                No
  Raps timeout timer is Running:        No
OS904#
```

## Node State

To view ERPS state information about the node:

1. Enter **enable** mode.
2. Invoke the command:
   **show erp node-state**

Example

```
OS904# show erp node-state
   ring      APS State      Event       RPL-Owner   Enable
------------------------------------------------------------
     1       Protecting   Local SF          Yes        Yes
OS904#
```

# **Chapter 10:** Rate Limiting of Flood Packets

## Definition

Rate Limiting of Flood Packets is a service for limiting the rate of *ingress* packets at ports that tend to flood the network. (To limit the rate of *egress* packets, the traffic shaping function, described in the section *Shaping* on page *375*, can be used.)

## Purpose

Rate Limiting is used to prevent excessively high packet rates at ports that are potentially hazardous to the operation of bridged networks.

## Applicability

Rate Limiting can be applied to flood packets such as unknown-unicast, multicast, broadcast, and TCP-SYN. It can be set to any value in the range 46.08 Kbps to 1 Gbps with 46.08 Kbps granularity.

Applying Rate Limiting to flood packets in effect also prevents traffic storms. Flood packets that exceed the set rate limit are discarded.

**Note**

Rate Limiting of flood packets is configured in bits-per-second and the rate calculation takes into account all the packet bytes (including Ethernet framing overhead consisting of preamble + SFD + IPG). This means that the rate limitation is done at the Layer 1 level.

## Configuration

To limit the rate of flood packets at one or more ports:

1. Enter **`configure terminal`** mode.
2. Select the types of flood packets whose rate is to be limited by invoking *one or more* of the following commands:

```
port flood-limiting unknown-unicast PORTS-GROUP|all
port flood-limiting multicast PORTS-GROUP|all
port flood-limiting broadcast PORTS-GROUP|all
port flood-limiting tcp-syn PORTS-GROUP|all
port flood-limiting extra unknown-unicast PORTS-GROUP|all
port flood-limiting extra multicast PORTS-GROUP|all
port flood-limiting extra broadcast PORTS-GROUP|all
port flood-limiting extra tcp-syn PORTS-GROUP|all
```

where,

**`port`**: Action on port.

**`flood-limiting`**: The flood/rate limiting mechanism.

**`unknown-unicast`**: Unknown unicast packets.

**`multicast`**: Multicast packets.

**`broadcast`**: Broadcast packets.

**`tcp-syn`**: TCP SYN (OSI Layer 4) packets

**`PORTS-GROUP`**: Group of ports (to which rate-limiting is to be applied).

**`all`**: All ports (to which rate-limiting is to be applied).

**extra**: This argument is used to distinguish a second packet type for the same port (or group of ports). For instance, suppose that for a specific port (e.g., Port **3**) a packet type is defined (e.g., **unknown-unicast**) and the rate is set (e.g., **10m**). To define a different packet type and to set a rate for it for the *same* port use the argument **extra**. The example at the end of this chapter demonstrates its use. Note that the same packet type must not be included in two commands that differ only in the argument **extra**.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# port flood-limiting tcp-syn 1-3
OS900(config)#
```

3. Set the rate limit for the types of flood packets selected in Step *2* by invoking one or both of the following command:

   **port flood-limiting rate VALUE PORTS-GROUP|all**

   **port flood-limiting extra rate VALUE PORTS-GROUP|all**

   where,

   **port**: Action on port.

   **flood-limiting**: *Without* the keyword **extra**, the flood/rate limiting mechanism to be applied to the packet type selected using any of the first four commands in Step *2*, above.

   **extra**: Extra flood-limit. The flood/rate limiting mechanism to be applied to the packet type selected using any of the last four commands in Step *2*, above. This option is needed when for the same port (or group of ports) *one rate* is to be applied to one set of packet types while *another rate* is to be applied to another set of packet types. Note that the same packet type may not be included in both sets. See the example below demonstrating use.

   **rate**: Permitted rate per port.

   **VALUE**: Rate to which the selected set of packet types are to be limited at each port in the group to be subjected to rate limiting of flood packets. The minimum rate selectable is as follows:

   If the argument 'extra' is *included* in the command: 2.03m bps

   If the argument 'extra' is *not included* in the command:

   For a 10/100 Mbps port: 202.75k bps

   For a 1000 Mbps port: 2.03m bps

   The maximum rate selectable is 1 Gbps.

   If a value that is not an integral multiple of 46.08k bps is entered, the OS900 automatically sets the rate to an integral multiple of the granularity 46.08k bps that is closest to the value entered by the user. Examples of values that can be entered are: **800k**, **50m**, and **1g**. The rate applies to the packet types collectively.

   **PORTS-GROUP**: Group of ports (to which rate-limiting is to be applied).

   **all**: All ports (to which rate-limiting is to be applied).

Example

This example demonstrates configuration of rate limiting of flood packets.

Suppose the following are required:

- Application of rate limiting of flood packets to Port 3 and Port 4.
- The rate for *broadcast packets* and *multicast* packets (collectively) are to be limited to 600k bits/sec.
- The rate for *unknown unicast packets* and *TCP SYN (OSI Layer 4) packets* (collectively) are to be limited to 3m bits/sec.

Note that a specific packet type (*broadcast,* etc.) is not included for both rates.

```
OS900(config)# port flood-limiting multicast 3,4
OS900(config)# port flood-limiting broadcast 3,4
OS900(config)# port flood-limiting rate 600k 3,4
Set rate to 600k bit/sec

OS900(config)# port flood-limiting extra unknown-unicast 3,4
OS900(config)# port flood-limiting extra tcp-syn 3,4
OS900(config)# port flood-limiting extra rate 3m 3,4
Set rate to 3m bit/sec
OS900(config)#
```

In the above example, the rate entered by the user is **`600k`** `bit/sec`. However, the OS900 sets the rate to `599.04k bit/sec` because it is an integral multiple of the granularity 46.08 Kbps that is closest to the rate **`600k`** `bit/sec`.

# Viewing

To view the rate limit configured for one or more ports, invoke the command:

**`show port flood-limiting`**

Example

```
OS900# show port flood-limiting
port flood-limiting rate 599.04k 3-4
port flood-limiting multicast 3-4
port flood-limiting broadcast 3-4
port flood-limiting extra rate 3m 3-4
port flood-limiting extra unknown-unicast 3-4
port flood-limiting extra tcp-syn 3-4
OS900#
```

# Deleting

To cancel rate limiting of flood packets, enter **`configure terminal`** mode and invoke one or more of the following commands:

**`no port flood-limiting PORTS-GROUP|all`**
**`no port flood-limiting [rate] PORTS-GROUP|all`**
**`no port flood-limiting [unknown-unicast] PORTS-GROUP|all`**
**`no port flood-limiting [multicast] PORTS-GROUP|all`**
**`no port flood-limiting [broadcast] PORTS-GROUP|all`**
**`no port flood-limiting [tcp-syn] PORTS-GROUP|all`**

where,

**`no`**: Cancel.
**`port`**: Action on port.
**`flood-limiting`**: The flood/rate limiting mechanism.
**`[unknown-unicast]`**: Unknown unicast packets.
**`[multicast]`**: Multicast packets
**`[broadcast]`**: Broadcast packets
**`[tcp-syn]`**: TCP SYN (OSI Layer 4) packets
**`[rate]`**: Rate set for port(s).
**`PORTS-GROUP`**: Group of ports (for which rate-limiting is to be cancelled).
**`all`**: All ports (for which rate-limiting is to be cancelled).

If only the *type(s)* of packet is used in the above commands, rate-limiting will be cancelled for the selected type(s) on the port. However, the *rate* configured for the port is retained.

If only the *rate* for a port is used in the above commands, rate-limiting will be cancelled for the port. However, the *type(s)* of packet configured for the port is retained.

If *neither* the *type(s)* of packet *nor* the *rate* for a port is used in the above commands, rate-limiting will be cancelled for the port. In addition, the *type(s)* of packet as well as the *rate* configured for the port are deleted.

Example

```
OS900(config)# no port flood-limiting rate 1,3
OS900(config)#
```

# Example

The following example is provided to show the scope of the 'Rate Limiting of Flood Packets' mechanism.

Suppose the following are required:

– Rate Limiting of Flood Packets is to be applied to Port 3.

– Two sets of packet types are to be distinguished. The first set is to contain the types **unknown-unicast** and **multicast**. The second set is to contain only the type **tcp-syn**.

– The rate limit to be applied to the first set is 10 Mbps.

– The rate limit to be applied to the second set is 20 Mbps.

```
--------------------------Setting the Flood Packet Types and Rate Limits for Port 3--------------------------

OS910> enable
OS910# configure terminal
OS910(config)# port flood-limiting unknown-unicast 3
OS910(config)# port flood-limiting multicast 3
OS910(config)# port flood-limiting extra tcp-syn 3
OS910(config)# port flood-limiting rate 10m 3
Set rate to 10m bit/sec
OS910(config)# port flood-limiting extra rate 20m 3
Set rate to 20m bit/sec

--------------------------------------------------Viewing the Setting--------------------------------------------------

OS910(config)# do show port flood-limiting
port flood-limiting rate 10m 3
port flood-limiting unknown-unicast 3
port flood-limiting multicast 3
port flood-limiting extra rate 20m 3
port flood-limiting extra tcp-syn 3
OS910(config)#
```

# Chapter 11: Provider Bridges

## General

A Provider Bridge (Service VLAN, VMAN, Stacked VLAN, or Q-in-Q) is an IEEE 802.1ad standard mechanism that uses an extra service provider tag as part of the Ethernet frame header in order to provide IEEE 802.1Q standard VLAN interconnectivity between remote sites of a customer scattered across a service provider network.

Provider Bridges provide separate instances of MAC services to multiple independent users of a carrier network (shared service provider network). Each instance is an interconnection of several sites of the same customer that are distributed across a carrier network. The interconnection is made possible using the same VLAN ID for the sites. The VLAN ID encapsulates the customer VLAN frames. The carrier network is utilized as a completely transparent transport medium between the sites so that the sites appear to be *directly* interconnected.

In order to enable transparency for customer services, described above, a provider bridge should be able to tunnel Layer 2 control protocol packets across the carrier network. This feature of a provider bridge is described in detail in the section *Tunneling of Layer 2 Protocols*, page *257*. For example, a group of sites can be bridged into one VLAN under a single MSTP domain.

## Purpose

The purpose of Provider Bridges is twofold:

1) To isolate different types of traffic from one another (on the basis of service and/or customer) in a manner that is transparent to traffic of the same customer VLAN.
2) To bridge customers or groups of customers scattered across the service provider network

A Provider Bridge fulfills these purposes without interfering with the client VLAN structure while “hiding” the internal VLAN structure of the customer network from others.

## Number of Provider Bridges

The maximum number of Provider Bridges that can be configured is 4K.

## Provider Bridge Ethertype

A Provider Bridge Ethertype (TPID[23]) is a value in the *hex* range 0 to FFFF. Two Provider Bridge Ethertype values can be set for the OS900. Either Provider Bridge Ethertype can be set for each OS900 *core* port[24] independently. If no Ethertype is set for a core port, by default, the OS900 uses the IEEE 802.1Q standard Ethertype 0x8100 for the port. The default Ethertype for 802.1ag CCM packets is 0x8902.

## Provider Bridge Tag

A Service VLAN (Provider Bridge) tag is a second (outer) IEEE 802.1Q standard VLAN tag and has a value in the *decimal* range 0 to 4095.

## Principle of Operation

A packet (tagged or untagged) entering an *access* port is directed to a *core* port or to another access port. At the core port, the packet is pushed with another VLAN header that includes the Service VLAN Ethertype (pre-assigned by the user to the core port) and Service VLAN tag (VLAN

[23] The IEEE 802.1ad standard refers to a Service VLAN Ethertype as TPID (Tag Protocol IDentification).

[24] *Core* port is also known as *provider network* port.

interface tag assigned to the packet) and then forwarded on the provider network to the other access ports of the same customer.

A packet entering a *core* port from the provider network is forwarded to the access port whose VLAN tag matches Service VLAN tag of the packet. The access port pops the Service VLAN header (Service VLAN Ethertype and Service VLAN tag) and forwards the packet on the access network.

# Configuration

To configure access and core ports to operate in Service VLAN mode:

1. Enter **`configure terminal`** mode.
2. Ensure that the ports are members of a VLAN interface. (*Configuring*, page *181*, shows how to configure a VLAN interface. The configuration example at the end of this chapter also shows how to configure a VLAN interface.) This VLAN interface is the Service VLAN.
3. Set each *core* (provider network) port of the OS900 that is to participate in the Service VLAN, using the following command:

   **`port tag-outbound-mode tagged PORTS-GROUP`**

   where,

   **`port`**: Port configuration

   **`tag-outbound-mode`**: Mode for egress packets

   **`tagged`**: Tagged egress packets. (This setting is required for Service VLAN *core* ports.)

   **`PORTS-GROUP`**: Group of Ports

   Example

```
OS900(config)# port tag-outbound-mode tagged 3-4
OS900(config)#
```

4. Set each *access* (provider edge) port of the OS900 that is to participate in the Service VLAN, using the following command:

   **`port tag-outbound-mode q-in-q PORTS-GROUP TAG`**

   where,

   **`port`**: Port configuration.

   **`tag-outbound-mode`**: Mode for egress packets

   **`q-in-q`**: Untagging of egress packets. (This setting is required for Service VLAN *access* ports.)

   **`PORTS-GROUP`**: Group of Ports

   **`TAG`**: The default Service tag to be set for all packets entering the port

   Example

```
OS900(config)# port tag-outbound-mode q-in-q 2 92
OS900(config)#
```

   An access port can be a member of several Service VLANs. Packets entering the access port will be assigned, by default, the Service VLAN tag set in the above command. In the above example, packets entering port 2 will be assigned, by default, Service VLAN tag 92. Packets entering the port can be switched to another Service VLAN instead of the default Service VLAN by the action **`action tag swap <0-4095>`** in an ACL rule. For details, refer to the section *Stage 2 – Actions on Packet*, page *304.*

5. [If only the default Service VLAN Ethertype (**0x8100**) is to be used, skip this step.] Define the Service VLAN Ethertypes using the command:

   **`vman core-ethertype-1 ETHERTYPE core-ethertype-2 ETHERTYPE`**

   where,

   **`vman`**: Service VLAN configuration.

   **`core-ethertype-1`**: First Service VLAN Ethertype.

   **`ETHERTYPE`**: (first) First Service VLAN Ethertype value in hexadecimal code.

**core-ethertype-2**: Second Service VLAN Ethertype.

**ETHERTYPE**: (second) Second Service VLAN Ethertype value in hexadecimal code.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# vman core-ethertype-1 9100 core-ethertype-2 8c5a
OS900(config)#
```

6. [If only the default Service VLAN Ethertype (**0x8100**) is to be used, skip this step.] To each OS900 port connected to the provider network, assign either of the two Service VLAN Ethertypes by invoking the command:

   **port core-ethertype-1|core-ethertype-2 PORTS-GROUP**

   where,

   **port**: Port configuration.

   **core-ethertype-1**: First Service VLAN Ethertype value.

   **core-ethertype-2**: Second Service VLAN Ethertype value.

   **PORTS-GROUP**: Group of ports.

Example

```
OS900(config)# port core-ethertype-1 1,2
OS900(config)#
```

# Viewing

To view Service VLAN Ethertype configuration:

1. Enter **enable** mode.
2. Invoke the command **show vman**

Example

```
OS900# show vman
Value of ethertype 1 is 0x8100 (default value)
Value of ethertype 2 is 0x8100 (default value)
Core ports with ethertype=1 (default port ethertype): 1-4
OS900#
```

# Example

The purpose of the example here is to show how Service VLANs, in general, can be configured. For simplicity, only three Service VLANs are configured. However, this number should be sufficient to indicate the scope of Service VLAN configuration.

## Application Description

Ports 1 and 2 are *access* ports belonging to customers 1 and 2, respectively. Ports 3 and 4 are *core* ports.

Two Service VLANs are configured: 91 and 92 (A Service VLAN is actually configured in the same way as any VLAN interface.) Customer 1 will be assigned to Service VLAN tag 91, Customer 2 will be assigned to Service VLAN tag 92.

## Packet Data Path and Processing

Packets from the *access* port 1 are assigned to Service VLAN 91 and forwarded to the core ports 3 and 4. Here, each packet (whether tagged or untagged) is pushed[25] with the Service VLAN tag 91 and forwarded on the provider network.

[25] Pushing the Service VLAN packet means adding another 802.1Q header that includes the default Service VLAN Ethertype 0x8100 and the Service VLAN tag. The Ethertype added to this header may be set to a value that is different

Packets from the *access* port 2 are assigned to Service VLAN 92 and forwarded to the core ports 3 and 4. Here, each packet (whether tagged or untagged) is pushed with the Service VLAN tag 92 and forwarded on the provider network.

Packets entering *core* port 3 or 4 from the provider network are checked. If the Service VLAN tag (outer tag) is 91, the packet is directed to access port 1. (Actually, the packet is forwarded as a tagged packet on Service VLAN 91.) If the Service VLAN tag is 92, the packet is directed to access port 2. Otherwise, the packet is dropped. At ports 1 and 2, the Service VLAN header (Ethertype and tag) is popped and the packet is forwarded to the network of customers 1 and 2, respectively.

## Configuration

The following is an example showing how service VLANs can be configured:

- Setting core ports 3 and 4 to tagged mode
- Specification of Service VLAN interface containing Ports 1, 3 and 4 (tag 91, default Service VLAN for access port 1)
- Specification of Service VLAN interface containing Ports 2, 3 and 4 (tag 92, default Service VLAN for access port 2)
- Setting access ports 1 and 2 to q-in-q mode, and setting its default Service VLANs (91 and 92).

```
MRV OptiSwitch 910 version d1320-22-08-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
OS900(config)# port tag-outbound-mode tagged 3,4
OS900(config)# interface vlan vif91
OS900(config-vif1)# ports 1,3,4
OS900(config-vif1)# tag 91
Interface is activated.
OS900(config-vif1)# exit
OS900(config)#
OS900(config)# interface vlan vif92
OS900(config-vif2)# ports 2,3,4
OS900(config-vif2)# tag 92
Interface is activated.
OS900(config-vif2)# exit
OS900(config)#
OS900(config)#
OS900(config)# port tag-outbound-mode q-in-q 1 91
OS900(config)# port tag-outbound-mode q-in-q 2 92
OS900(config)# exit
OS900#
```

## Extending the Application

Packets entering access Port 2, in the above example, can be assigned to a Service VLAN based on the customer VLAN tag. In the extended example below, a packet entering Port 2 with customer tag 10 will be assigned to a new Service VLAN 102. All other packets will still be assigned to the port's default Service VLAN 92.

Such an application is useful when a single access port receives traffic from more than one customer (e.g., when a DSLAM is connected on the access port), or when the customer connected to the access port requires several Service VLANs and not just one (e.g., a Service VLAN per service type, such as, for e.g., voice, video, or data).

---

from the default by assigning a different *core ethertype* to the core ports using the commands `vman core-ethertype` and `port core-ethertype`.

## Extended Configuration

The extended configuration includes:

- Specification of another Service VLAN interface containing Ports 2, 3, and 4 (service tag 102).
- Defining an ACL that classifies packets according to the customer tag 10 and swaps the tag with the new Service VLAN tag 102.
- Binding the ACL to the access port as described in the section *Binding*, page *316*.

```
MRV OptiSwitch 910 version d1320-22-08-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
OS900(config)# interface vlan vif102
OS900(config-vif1)# ports 2,3,4
OS900(config-vif1)# tag 102
Interface is activated.
OS900(config-vif1)# exit
OS900(config)#
OS900(config)# access-list extended svlan102
OS900(config-access-list)# rule 10
OS900(config-rule)# tag eq 10
OS900(config-rule)# action tag swap 102
OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)#
OS900(config)# port acl-binding-mode by-port 2
OS900(config)# port access-group svlan102 2
OS900(config)#
```

# Tunneling of Layer 2 Protocols

## General

Tunneling of Layer 2 Protocols uses Service VLANs (see ***Chapter 11:*** *Provider Bridges*, page *253*) to tunnel protocol packets across a provider network without affecting the provider, e.g., without network reconfiguration by customer MSTP packets.

**Note**

STP traffic (BPDUs) from ports configured as tunnel ports do not participate in the OS900 MSTP, but are tunneled through the service VLAN.

In this method of tunneling, the destination MAC address is changed.

There are currently two models for implementing Tunneling of Layer 2 Protocols:

- Cisco Layer 2 Protocol Tunneling
- IEEE 802.1ad Provider Bridges Tunneling

The OS900 uses Cisco's model and is, therefore, compatible with Cisco devices.

Using the osL2PduGuard.MIB with an SNMP Manager, up to two threshold levels can be set up per port and the state of each port can be viewed. By default, all storm guard thresholds are disabled.

## Principle of Operation

The principle of operation is based on Cisco's L2PT.

Layer 2 PDUs entering an Edge switch from its access (customer) side have their Destination MAC address changed to a special MAC address. This new MAC address makes the PDUs appear as ordinary data packets to the carrier network. The PDUs are then forwarded on the carrier network using their VLAN ID. Core switches in the carrier network forward these PDUs to the Edge switches at the other sites of the customer without processing them. The PDUs at these switches have their Destination MAC address changed back to the previous Destination MAC address, and identical copies are delivered to all customer ports in the same VLAN.

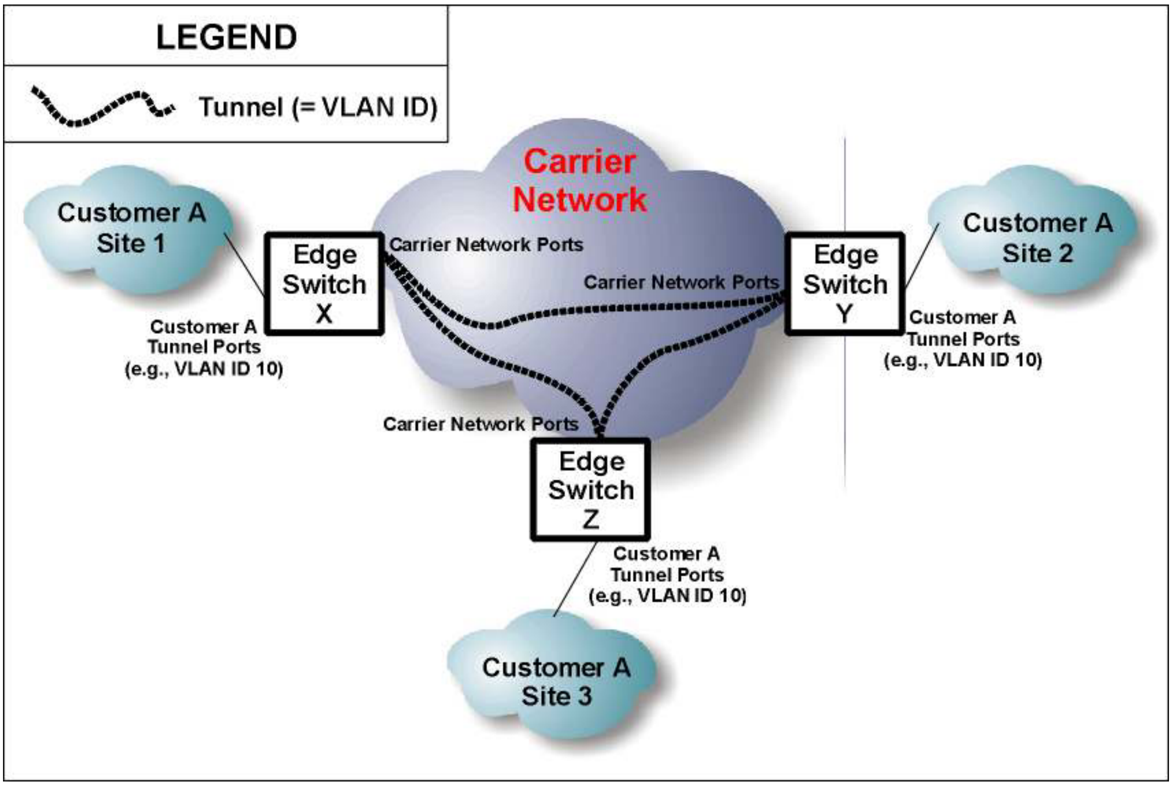



**Figure 32: Layer 2 Protocol Tunneling**

## Configuration

The procedure for configuring edge OS900s (that have ports connected to the sites of a customer) to provide Layer 2 tunneling over a carrier network is as follows:

At *each* customer site (OS900 site):

1. Connect the customer 802.1Q VLAN trunk ports to the Edge OS900 ports (called tunnel ports).
2. Create a VLAN (as described in ***Chapter 7:*** *Interfaces*, page *177*) on the Edge OS900 that includes the tunnel ports.
3. To tunnel one or more protocols on one or more ports, in **`configure terminal`** mode, invoke the command:

    **`port l2protocol-tunnel (all|cdp|pvst+|stp|vtp|dtp|pagp|udld|lacp|lamp|efm|dot1x|elmi|lldp|garp) PORTS-GROUP [drop]`**

    where,

    **`all`**: All protocol datagrams, i.e., **`cdp`**, **`pvst+`**, **`stp`**, **`vtp`**, **`dtp`**, **`pagp`**, **`udld`**, and **`lacp`**

    **`cdp`**: Cisco discovery protocol datagrams

    **`pvst+`**: Cisco Per VLAN Spanning Tree Plus discovery protocol datagrams. (PVST+ provides the same functionality as PVST. PVST uses ISL trunking technology whereas PVST+ uses IEEE 802.1Q trunking technology.

    PVST functionality is as follows:

    It maintains a spanning tree instance for each VLAN configured in the network. It allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each

VLAN as a separate network, it has the ability to load balance traffic (at OSI Layer 2) by enabling forwarding for some VLANs on one trunk and enabling forwarding for other VLANs on another trunk, without causing a Spanning Tree loop.

**stp**: IEEE 802.1w or IEEE 802.1s spanning-tree protocol datagrams

**vtp**: IEEE 802.3ad VLAN trunk protocol datagrams

**dtp**: Dynamic Trunking Protocol

**pagp**: Port Aggregation Protocol

**udld**: Uni-Directional Link Detection Protocol

**lacp**: IEEE 802.3ad Link Aggregation Control Protocol (LACP) datagrams

**lamp**: Location Aware MAC Protocol

**efm**: Ethernet in the First Mile 802.3ah protocol

**dot1x**: Port Authentication IEEE 802.1x protocol

**elmi**: Ethernet Local Management Interface protocol

**lldp**: Link Layer Discovery Protocol

**garp**: GARP Multicast Registration Protocol

**PORTS-GROUP**: Group of ports to be configured as tunnel ports

**[drop]**: Drop packets

Example

```
OS900(config)# port l2protocol-tunnel cdp 3
OS900(config)#
```

(To cancel tunneling of one or more protocols on one or more ports , invoke the command: **no port l2protocol-tunnel (all|cdp|pvst+|stp|vtp|dtp|pagp|udld|lacp|lamp|efm|dot1x|elmi|lldp|garp) [PORTS-GROUP]** )

4. [Optional] Define the MAC address of the destination of the packets for which the protocol/s have been specified in Step *3*, above, by invoking the command:

   **l2protocol-tunnel mac MAC_ADDRESS**

   where,

   **MAC_ADDRESS**: MAC address in the format **01:xx:xx:xx:xx:xx**, where **xx** is a double-digit hexadecimal number

   (To revoke the defined MAC address of the destination, invoke the command: **no l2protocol-tunnel mac**.)

5. [Optional] To activate the storm guard mechanism (i.e., to notify and, optionally, isolate/disable a port that receives PDUs at a rate that is in excess of the set limit), invoke the command:

   **l2-pdu-storm-guard protocol (all|cdp|dtp|pagp|efm|dot1x|esmc|lacp|pvst+|stp|vtp|udld|ethoam|erp) port (PORTS-GROUP|all) <0-1000> [inform <0-1000>]**

   where,

   **all**: All protocol datagrams, i.e., **cdp**, **pvst+**, **stp**, **vtp**, **dtp**, **pagp**, **udld**, and **lacp**

   **cdp**: Cisco discovery protocol datagrams

   **dtp**: Dynamic Trunking Protocol

   **pagp**: Port Aggregation Protocol

   **efm**: Ethernet in the First Mile 802.3ah protocol

   **dot1x**: Port Authentication IEEE 802.1x protocol

   **esmc**: Ethernet Synchronization Messaging Channel protocol

   **lacp**: IEEE 802.3ad Link Aggregation Control Protocol (LACP) datagrams

   **pvst+**: Cisco Per VLAN Spanning Tree Plus discovery protocol datagrams. (PVST+ provides the same functionality as PVST. PVST uses ISL trunking technology whereas PVST+ uses IEEE 802.1Q trunking technology.

PVST functionality is as follows:

It maintains a spanning tree instance for each VLAN configured in the network. It allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each VLAN as a separate network, it has the ability to load balance traffic (at OSI Layer 2) by enabling forwarding for some VLANs on one trunk and enabling forwarding for other VLANs on another trunk, without causing a Spanning Tree loop.

**stp**: IEEE 802.1w or IEEE 802.1s spanning-tree protocol datagrams

**vtp**: IEEE 802.3ad VLAN trunk protocol datagrams

**udld**: Uni-Directional Link Detection Protocol

**ethoam**: Ethernet Operations, Administration and Maintenance protocol

**erp**: Ethernet Ring Protection protocol

**<0-1000>**: (First appearance) Maximum number of PDUs per port per second allowed above which the port(s) are to be isolated/disabled. To disable the storm guard mechanism, select **0**. (Default: **50** packets per second for any port.)

**<0-1000>**: (Second appearance) Maximum number of PDUs per port per second allowed above which notification is to be sent . To disable the storm guard mechanism, select **0**. (Default: **50** packets per second for any port.)

**PORTS-GROUP**: Group of ports for which the storm guard mechanism is to be activated.

To deactivate the storm guard mechanism, invoke the command:

**no l2-pdu-storm-guard protocol (all|cdp|dtp|pagp|efm|dot1x|esmc|lacp|pvst+|stp|vtp|udld|ethoam|erp) port (PORTS-GROUP|all)**

To view the protocols for which the storm guard mechanism will block ports, invoke the command:

**show l2-pdu-storm-guard protocol (all|cdp|dtp|pagp|efm|dot1x|esmc|lacp|pvst+|stp|vtp|udld|ethoam|erp) port (PORTS-GROUP|all)**

## Viewing

To display the tunneling configuration:

1. Enter **enable** mode.
2. Invoke the command:

   **show port l2protocol-tunnel**

Example

```
OS900(config)# do show port l2protocol-tunnel
STP tunnel-ports:
CDP tunnel-ports: 3
VTP tunnel-ports:
OS900(config)#
```

## Canceling

To cancel tunneling on one or more ports:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no port l2protocol-tunnel (all|cdp|pvst+|stp|vtp|dtp|pagp|udld|lacp|lamp|efm|dot1x|elmi|lldp|garp) [PORTS-GROUP]**

   where,

**all**: All protocol datagrams, i.e., **cdp**, **pvst+**, **stp**, **vtp**, **dtp**, **pagp**, **udld**, and **lacp**

**cdp**: Cisco discovery protocol datagrams

**pvst+**: Cisco Per VLAN Spanning Tree Plus discovery protocol datagrams. (PVST+ provides the same functionality as PVST. PVST uses ISL trunking technology whereas PVST+ uses IEEE 802.1Q trunking technology.

PVST functionality is as follows:

It maintains a spanning tree instance for each VLAN configured in the network. It allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each VLAN as a separate network, it has the ability to load balance traffic (at OSI Layer 2) by enabling forwarding for some VLANs on one trunk and enabling forwarding for other VLANs on another trunk, without causing a Spanning Tree loop.

**stp**: IEEE 802.1w or IEEE 802.1s spanning-tree protocol datagrams

**vtp**: IEEE 802.3ad VLAN trunk protocol datagrams

**dtp**: Dynamic Trunking Protocol

**pagp**: Port Aggregation Protocol

**udld**: Uni-Directional Link Detection Protocol

**lacp**: IEEE 802.3ad Link Aggregation Control Protocol (LACP) datagrams

**lamp**: Location Aware MAC Protocol

**efm**: Ethernet in the First Mile 802.3ah protocol

**dot1x**: Port Authentication IEEE 802.1x protocol

**elmi**: Ethernet Local Management Interface protocol

**lldp**: Link Layer Discovery Protocol

**garp**: GARP Multicast Registration Protocol

**PORTS-GROUP**: Group of ports to be configured as tunnel ports

Example

```
OS900(config)# no port l2protocol-tunnel cdp 3
OS900(config)#
```

# Tunneling/Dropping of STP BPDUs by Hardware

## General

In this method of tunneling, the destination MAC address is *not* changed.

## Definition

Tunneling by hardware of STP BPDUs is the transparent transmission of BPDUs between customer sites across the provider's network at the hardware layer.

## Advantages

In this method, the OS900's CPU is not involved. This has the following advantages:

1. CPU is freed to perform other tasks.
2. Whatever the load on the CPU, BPDUs will not be dropped.
3. Processing is done at wire-speed

## Terminology

C-STP – Spanning tree domain/traffic of a Customer

S-STP – Spanning tree domain/traffic of a Service Provider

Access Port – A port in a Provider's bridge that is dedicated to a single Customer only

Uplink Port – A port in a Provider's bridge that is connected to another Provider's bridge

Edge Bridge (for a customer) – A Provider's bridge directly connected to the Customer device through an access port

BPDU – Bridge Protocol Data Unit (STP)

## Application

Tunneling/dropping by hardware of STP BPDUs is applied when:

- A high rate of C-STP BPDUs is received on the bridge access port, and
- The provider does *not* want to isolate this access port using the BPDU storm guard feature (described in the section *Storm Guard*, page *406*).

## C-STP BPDU Tunneling

### Enabling

To make the bridge[26] transparent to BPDUs[27] with tags (from the TAGS-LIST), invoke the command:

**`bpdu-tunnel-tag TAGS-LIST [uplink-ports PORTS-GROUP]`**

where,

**`TAGS-LIST`**: Group of BPDUs to be tunneled

**`PORTS-GROUP`**: Group of ports

If the optional parameter 'uplink-ports PORTS-GROUP' is used, the specified ports still participate in the S-STP in order to prevent loops. The other ports are flooded with BPDUs according to the VLAN as regular multicast frames.

### Disabling

To cause BPDUs with certain tags to be handled by the S-STP, invoke the command:

**`no bpdu-tunnel-tag TAGS-LIST [uplink-ports PORTS-GROUP]`**

where,

**`TAGS-LIST`**: Tags of BPDUs to be dropped

**`[uplink-ports PORTS-GROUP]`**: Group of uplink ports to prevent tunneling. If this argument is not used, BPDUs with the tags specified in **`TAGS-LIST`** will be dropped at all uplink ports.

## S-STP BPDU Transmission

### Disabling

To disable sending of S-STP BPDUs to the C-STP domain, invoke the command:

**`port PORTS-GROUP disable-bpdu-tx`**

where,

**`PORTS-GROUP`**: Group of (uplink) ports via which S-STP BPDUs are not to be sent to the C-STP

It is a good policy to define this mode on access ports.

### Enabling

To enable sending of S-STP BPDUs to the C-STP domain, invoke the command:

**`no port PORTS-GROUP disable-bpdu-tx`**

where,

**`PORTS-GROUP`**: Group of (uplink) ports via which S-STP BPDUs are not to be sent to the C-STP

---

[26] OS900

[27] Usually C-STP BPDUs

## C-STP BPDU Dropping/Forwarding

### Dropping

To drop C-STP BPDUs, invoke the following two commands:

```
bpdu-drop-tag TAGS-LIST
no bpdu-tunnel-tag
```

where,

**TAGS-LIST**: Tags of BPDUs to be dropped

### Forwarding

To foward C-STP BPDUs, invoke the following two commands:

```
no bpdu-drop-tag TAGS-LIST
bpdu-tunnel-tag
```

where,

**TAGS-LIST**: Tags of BPDUs to be forwarded

## Example

### Purpose

The example is used to show how to configure OS900s to tunnel and/or to drop BPDUs.

### Network

The network shows two *access side* switches **C1** and **C2** (possibly OS900s) and two *provider side* switches **S1** (OS900) and **S2** (OS900). The blue links are customer side downlinks. The red links are provider side uplinks.

At **S1**, BPDUs with tag 10 are to be transparent at uplink ports 3 and 4. Ports 1 and 2 are to be prevented from sending BPDUs to the provider's spanning-tree domain. BPDUs with tag 10 in the customer's spanning-tree domain are to be dropped.
At **S2**, BPDUs with tag 10 are to be transparent at uplink ports 1 to 4.

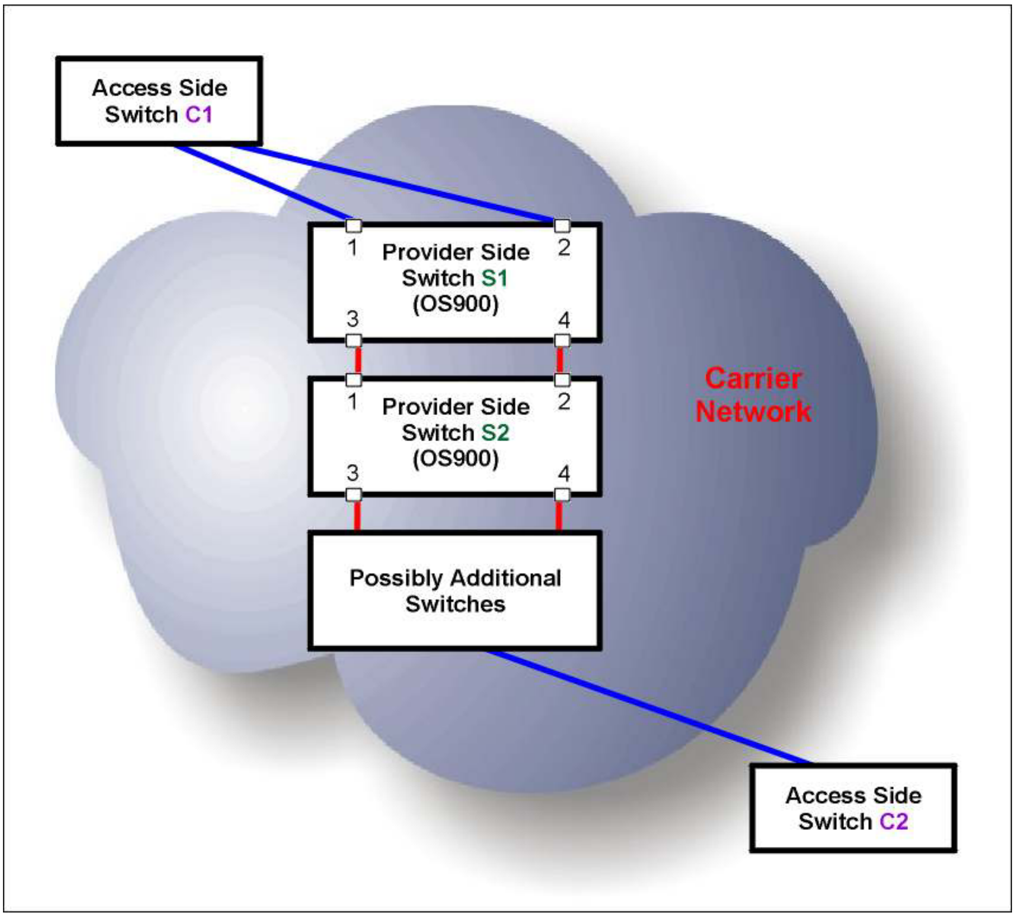



**Figure 33: Hardware Tunneling/Dropping of STP BPDUs – Example**

### Configuration

```
-------------------- S1 ------------------------------------------------------------
C(config)# spanning-tree
C(config-mstp)# bpdu-tunnel-tag 10 uplink-ports 3-4
C(config-mstp)# port 1-2 disable-bpdu-tx
C(config-mstp)# bpdu-drop-tag 10
C(config-mstp)#

-------------------- S2 ------------------------------------------------------------
C(config)# spanning-tree
C(config-mstp)# bpdu-tunnel-tag 10 uplink-ports 1-4
C(config-mstp)#
```

# Chapter 12: Tag Translation/Swapping

## Definition

Tag-translation/swapping is the translation & swapping of a packet's source VLAN tag at one UNI[28] with that of the destination VLAN tag at another UNI (so that the packet can be received at the destination).

## Purpose

Tag- translation/swapping, unlike tag-nesting (service provider bridges q-in-q operation per IEEE 802.1ad), is used to interconnect two LANs/CPEs, that are located at different UNIs and *do not have the same* VLAN tag[29], across an Ethernet metro network.

## Advantages

- VLAN tags at different UNIs can be assigned independently of each other
- Non-IP as well as IP packets can be delivered across an Ethernet metro network

## Application

Interconnection of the LANs/CPEs is done per ACL. This means that traffic flow between the CPEs can *also be fully controlled* (by the packet filtering capability of ACLs).

Both tagged and untagged frames are allowed at ingress. Packets received from the customer site are encapsulated with an additional tag (Service VLAN tag) before being forwarded over the Ethernet metro network. Packets received from the Ethernet metro network are stripped of the Service VLAN tag before they are forwarded to the customer site.

Following are application scenarios in which tag-translation/swapping is used:

- Interconnection of two LANs/CPEs of one customer that are located at different UNIs
- Tying two LANs/CPEs of two organizations that have merged across an Ethernet metro network
- Connecting different customers to the same Internet Service Provider (ISP)

## Point-to-Point Topology

This section describes, with the aid of an example, the principle of operation, configuration procedure, and implementation of the OS900 tag-translation/swapping mode for a point-to-point interconnection topology.

### Principle of Operation

The principle of operation in tag translation mode is explained with the aid of the example in *Figure 34*, below. At customer site **A**, VLAN Tag **10** of a packet entering an OS900 port that is a member of the VLAN *is translated into* Tag **20**, encapsulated with the service tag **700**, and sent over the network to the OS900 connecting customer site **B**. At the OS900, the packet is stripped of the service tag **700**, and sent to customer site **B**.

At customer site **B**, VLAN Tag **20** of a packet entering an OS900 port that is a member of the VLAN *is translated into* Tag **10**, encapsulated with the service tag **700**, and sent over the network

[28] User-to-Network Interface. The type of network considered here is Ethernet metro network.

[29] It is possible that the VLAN tags are different or that one CPE has a VLAN tag while the other does not.

to the OS900 connecting customer site **A**. At the OS900, the packet is stripped of the service tag **700**, and sent to customer site **A**.

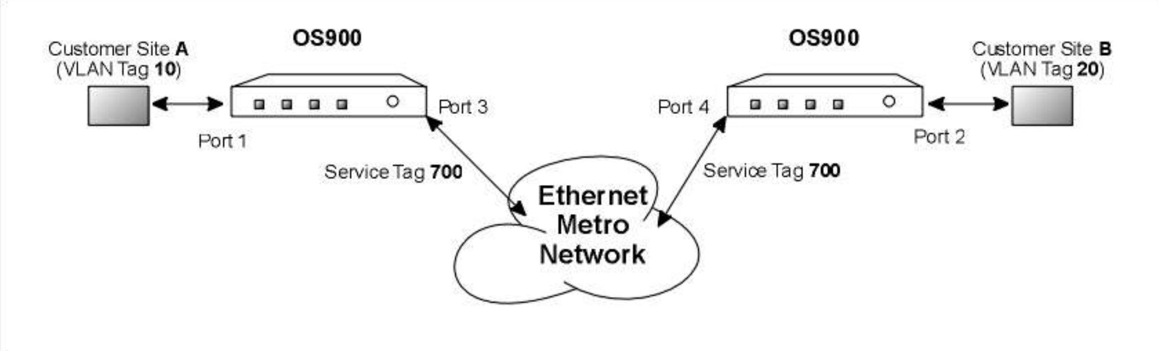



**Figure 34: Tag Translation Operation Mode for Point-to-point Topology**

## Configuration

To configure tag translation/swapping in order to interconnect *one pair* of LANs/CPEs, perform the following steps *for each of the two OS900s* (one at Customer Site A, the other at B):

1. Enter **`configure terminal`** mode.
2. Select a port to be set in untagged mode by invoking the command:
   **`port tag-outbound-mode untagged PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Customer port
3. Set untagged customer port to be a member of Multiple VLANs by invoking the command:
   **`port untagged-multi-vlans PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Customer port
4. Make the Customer Port and the Service Port members of an inband VLAN interface as described in the section *Configuring*, page *181*.

| | **Note** |
|---|---|
| | Assign the *same* tag to the two inband VLAN interfaces, one in the Customer Site A OS900 and the other in the Customer Site B OS900! |

5. Set VLAN Tag Swap Mode in an Access List by invoking the command:
   **`action tag swap-ctag <0-4095> stag <0-4095>`**
   where,
   **`<0-4095>`**: (First appearance) Range of *customer* VLAN tags from which one tag is to be selected.

   **`<0-4095>`**: (Second appearance) Range of *service* VLAN tags from which one tag is to be selected.
6. Bind the ACL to the customer port by invoking the commands:
   **`port acl-binding-mode by-port PORTS-GROUP`**
   **`port access-group WORD PORTS-GROUP`**
   where,
   **`PORTS-GROUP`**: Customer port
   **`WORD`**: Name of Access List
7. Set VLAN Tag Nesting Mode in a second Access List by invoking the command:
   **`action tag nest <0-4095>`**
   where,

**<0-4095>**: Range of *service* VLAN tags from which the *same* tag as in Step *4*, above, is to be selected. (Note that nest tag can be assigned to an internal port, external port, or VLAN.)

8. Bind the second Access List to the internal customer port having the same number as the port selected in Step 2, above, by invoking the command:

   **`port access-group extra WORD PORTS-GROUP`**

   where,

   **`WORD`**: Name of second Access List

   **`PORTS-GROUP`**: Customer port, other than port 11 or 12 of the OS912. The customer port can be a trunk port. (A trunk port is required to have the format **`tX`** where, **`X`** is a number in the range 1 to 9.)

9. Select the OS900 Service Port (UNI) connecting the Customer Site A by invoking the command:

   **`port tag-outbound-mode tagged PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Service port

**Note**

For each additional pair of LANs/CPEs to be interconnected, a different Service VLAN tag must be assigned.

## Implementation

The following example shows how to configure two OS900s to operate in Tag Translation mode across a network. Although port pairs with different numbers (namely, 1,3 and 2,4) are shown in the example, port pairs with the same numbers can be selected, e.g., 1,3 and 1,3.

**Configuring OS900 at Site A**

```
---------------------------------------Setting Customer Port 1 in Untagged Mode--------------------------------------

OS900(config)# port tag-outbound-mode untagged 1
OS900(config)#

--------------------Setting untagged Customer Port 1 to be a member of Multiple VLANs--------------------

OS900(config)# port untagged-multi-vlans 1
OS900(config)#

----------Making Customer Port 1 and Service Port 3 members of Inband VLAN Interface 700----------

OS900(config)# interface vlan vif83
OS900(config-vif83)# ports 1,3
OS900(config-vif83)# tag 700
Interface is activated.
OS900(config-vif83)#

---------------------------------Setting VLAN Tag Swap Mode in Access List ACL1--------------------------------

OS900(config)# access-list extended ACL1
OS900(config-access-list)# rule
OS900(config-rule)# action tag swap-ctag 20 stag 700
OS900(config-rule)#

---------------------------------------------Binding ACL1 to Customer Port 1--------------------------------------------

OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# port acl-binding-mode by-port 1
```

```
OS900(config)# port access-group ACL1 1
OS900(config)#
```

-----------------------------Setting VLAN Tag Nesting Mode in Access List ACL2-------------------------------

```
OS900(config)# access-list extended ACL2
OS900(config-access-list)# rule
OS900(config-rule)# action tag nest 700
OS900(config-rule)#
```

-------------------------------------Binding ACL2 to Internal Customer Port 1-------------------------------------

```
OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# port access-group extra ACL2 1
OS900(config)#
```

----------------------Selecting Service Port 3 at OS900 Connecting Customer Site A----------------------

```
OS900(config)# port tag-outbound-mode tagged 3
OS900(config)#
```

## Configuring OS900 at Site B

------------------------------------Setting Customer Port 2 in Untagged Mode------------------------------------

```
OS900(config)# port tag-outbound-mode untagged 2
OS900(config)#
```

--------------------Setting untagged Customer Port 2 to be a member of Multiple VLANs--------------------

```
OS900(config)# port untagged-multi-vlans 2
OS900(config)#
```

---------Making Customer Port 2 and Service Port 4 members of Inband VLAN Interface 700---------

```
OS900(config)# interface vlan vif83
OS900(config-vif83)# ports 2,4
OS900(config-vif83)# tag 700
Interface is activated.
OS900(config-vif83)#
```

--------------------------------Setting VLAN Tag Swap Mode in Access List ACL3--------------------------------

```
OS900(config)# access-list extended ACL3
OS900(config-access-list)# rule
OS900(config-rule)# action tag swap-ctag 10 stag 700
OS900(config-rule)#
```

-------------------------------------------Binding ACL3 to Customer Port 2-------------------------------------------

```
OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# port acl-binding-mode by-port 2
OS900(config)# port access-group ACL3 2
OS900(config)#
```

-----------------------------Setting VLAN Tag Nesting Mode in Access List ACL4-------------------------------

```
OS900(config)# access-list extended ACL4
```

```
OS900(config-access-list)# rule
OS900(config-rule)# action tag nest 700
OS900(config-rule)#

-------------------------------------Binding ACL4 to Internal Customer Port 2-------------------------------------

OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# port access-group extra ACL4 2
OS900(config)#

----------------------Selecting Service Port 4 at OS900 Connecting Customer Site A----------------------

OS900(config)# port tag-outbound-mode tagged 4
OS900(config)#
```

It is not required to select different customer port numbers and different service port numbers as in the example above. For instance, the customer port number at both OS900s could be selected as 1 and the service port number at both OS900s could be selected as 3.

As such, for the OS900 at site B ACL1 could be used instead of ACL3 and ACL2 could be used instead of ACL4.

# Point-to-Multipoint Topology

This section describes, with the aid of an example, the principle of operation and implementation of the OS900 tag-translation/swapping mode for a point-to-multipoint interconnection topology.

## Principle of Operation

The principle of operation in tag translation mode is explained with the aid of the example in *Figure 35*, below.

At customer site **A**, a packet entering an OS900 port with VLAN Tag **10** is encapsulated with the service tag **1000**, and sent over the network to the OS900 connecting customer site **B** or **C**. Whether the packet will reach customer site **B** or site **C** depends on the network's configuration. At the customer site **B** or **C**, the packet is stripped of  the service tag **1000** and its VLAN Tag **10** is *translated into* the appropriate tag; **30** for site **B**, **20** for site **C**.

The description for the handling of a packet entering an OS900 port at any of the other sites is similar.

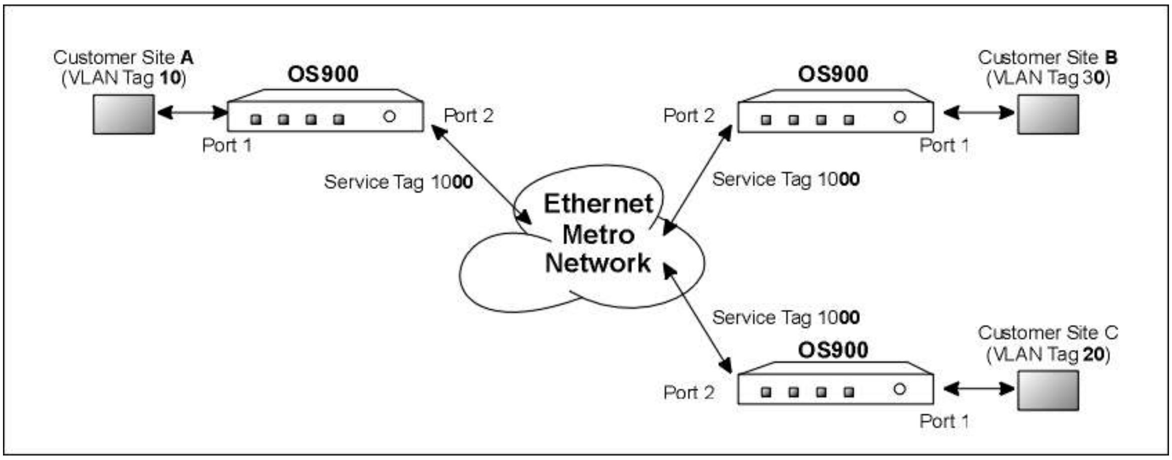



**Figure 35: Tag Translation Operation Mode for Point-to-Multipoint Topology**

## Implementation

**Configuring OS900 at Site A**

```
Site-A# show running-config
Building configuration...

Current configuration:
! version os900-3-1-0-D01-10-09-1626
!
hostname Site-A
!
line vty
 no exec-timeout global
!
access-list extended hybrid999
 default policy permit
 rule 10
  action tag swap 999
  tag eq 1000
!
access-list extended nest1000
 rule 10
  action tag nest 1000
  tag eq 10
!
access-list extended swap-ctag
 default policy permit
 rule 10
  action tag swap 10
  tag eq 20
 rule 20
  action tag swap 10
  tag eq 30
!
port tag-outbound-mode hybrid 2 999
port tag-outbound-mode tagged 1
!
port acl-binding-mode by-port 1-2
port access-group nest1000 1
port access-group hybrid999 2
port access-group egress swap-ctag 1
!
interface vlan vif10
 tag 10
 ports 1-2
!
interface vlan vif20
 tag 20
 ports 1-2
!
interface vlan vif30
 tag 30
 ports 1-2
!
interface vlan vif999
 tag 999
 ports 1-2
!
interface vlan vif1000
 tag 1000
 ports 1-2
!
no lt learning
!
Site-A#
```

## Configuring OS900 at Site B

```
Site-B# show running-config
Building configuration...

Current configuration:
! version os900-3-1-0-D01-10-09-1626
!
hostname Site-B
!
line vty
 no exec-timeout global
!
access-list extended hybrid999
 default policy permit
 rule 10
  action tag swap 999
  tag eq 1000
!
access-list extended nest1000
 rule 10
  action tag nest 1000
  tag eq 30
!
access-list extended swap-ctag
 default policy permit
 rule 10
  action tag swap 30
  tag eq 10
 rule 20
  action tag swap 30
  tag eq 20
!
port tag-outbound-mode hybrid 2 999
port tag-outbound-mode tagged 1
!
port acl-binding-mode by-port 1-2
port access-group nest1000 1
port access-group hybrid999 2
port access-group egress swap-ctag 1
!
interface vlan vif10
 tag 10
 ports 1-2
!
interface vlan vif20
 tag 20
 ports 1-2
!
interface vlan vif30
 tag 30
 ports 1-2
!
interface vlan vif999
 tag 999
 ports 1-2
!
interface vlan vif1000
 tag 1000
 ports 1-2
!
no lt learning
!
Site-B#
```

## Configuring OS900 at Site C

```
Site-C# show running-config
Building configuration...

Current configuration:
! version os900-3-1-0-D01-10-09-1626
!
hostname Site-C
!
line vty
 no exec-timeout global
!
access-list extended hybrid999
 default policy permit
 rule 10
  action tag swap 999
  tag eq 1000
!
access-list extended nest1000
 rule 10
  action tag nest 1000
  tag eq 20
!
access-list extended swap-ctag
 default policy permit
 rule 10
  action tag swap 20
  tag eq 10
 rule 20
  action tag swap 20
  tag eq 30
!
port tag-outbound-mode hybrid 2 999
port tag-outbound-mode tagged 1
!
port acl-binding-mode by-port 1-2
port access-group nest1000 1
port access-group hybrid999 2
port access-group egress swap-ctag 1
!
interface vlan vif10
 tag 10
 ports 1-2
!
interface vlan vif20
 tag 20
 ports 1-2
!
interface vlan vif30
 tag 30
 ports 1-2
!
interface vlan vif999
 tag 999
 ports 1-2
!
interface vlan vif1000
 tag 1000
 ports 1-2
!
no lt learning
!
Site-C#
```

# Chapter 13: IEEE 802.3ad Link Aggregation (LACP)

## Definition

Link Aggregation (Port Trunking) is the parallel interconnection of two or more ports to form a single logical communication channel whose bandwidth is the sum total of the bandwidths of the individual ports. Implementation is compliant to IEEE 802.3ad Link Aggregation Control Protocol (LACP) standard so that ports are automatically included or excluded at either end of a trunk so that the bandwidths of the two port groups at either end of the trunk are equal.

## Purpose

A Port Trunk between two switches increases traffic throughput capacity among stations connected to ports that are members of the trunk. For example, the interconnection of eight full-duplex Gigabit ports of one OS900 to eight full-duplex Gigabit ports of another OS900, serves as an 8-Gbps full-duplex Ethernet trunk.

In addition to increased link capacity, link aggregation results in higher link availability. It prevents the failure of any single link from leading to a disruption of communication between two OS900s.

## Number

The maximum number of port trunks that can be configured is by including just two ports per trunk.

For example, for the OS904 up to *two* port trunks can be configured and for the OS912 up to *six* port trunks can be configured.

## Types

There are two types of LACP:

- LACP
- Rapid LACP (MRV proprietary)

Both types send a packet every second. However, in LACP the LACP session comes up after 3 packets are received whereas in Rapid LACP the LACP session comes up immediately after 1 packet is received.

# Principle of Operation

### Frame Transfer

When LACP is enabled at both OS900s of the trunk, the OS900s dynamically exchange configuration information (e.g., presence and capabilities of the group members) between them. The OS900 compares the information it receives from the peer OS900 with its own setup, and accordingly dictates which ports are to be aggregated.

The LACP always tries to aggregate the maximum number of compatible ports in a trunk allowed by the hardware.

When LACP is not able to aggregate all the ports that are compatible (for example, the peer allows a smaller number of ports in a trunk), then all the ports that are not actively included in the aggregation are set in standby state.

A member port is excluded from a trunk when, for example, the Tx output of a port fails. In such case the Rx of the port at the other end of the trunk will not receive. As a result, the LACP will detect the failure and will reconfigure the trunk to exclude the port with the failed Tx output.

Traffic is distributed among the ports of a trunk according to the L2 addresses and L3 addresses of packets.

A Port Trunk transmits all unknown, broadcast, and multicasts packets, including BPDUs (which are multicast frames), via one port only.

### MSTP Action

All ports of a Port Trunk participate as just one port in MSTP. A Port Trunk functions as a single port.

## Rules

The following rules must be applied when configuring a Port Trunk:

1. All ports to be included in a trunk must have the default configuration. In particular, each port must be *untagged*.
2. Each Port Trunk must be formed with two or more ports.
3. The maximum number of port trunks that can be configured is by including just two ports per trunk.
4. A Port Trunk may consist of fixed ports and pluggable (SFPs/XFPs) ports.
5. A port that has been configured as an analyzer port cannot be a member of a Port Trunk.
6. A port may be a member of only one Port Trunk.
7. Each port to be included in the trunk must be untagged.
8. Except in *Link Protection* (page *139*), a trunk port may be connected only to a trunk port of another switch.
9. *One* trunk port on one OS900 may be connected to any *one* (and only one) trunk port on another OS900.
10. To be able to modify or delete a Port Trunk of an OS900 participating in MSTP, all member ports that have an active link must first be disconnected.

## Configuration

To configure a Port Trunk:

1. Enter **`configure terminal`** mode.
2. To create a port trunk, invoke the command:

   **`port trunk NAME PORTS-GROUP`**

   where,

   **`port`**: Port action.

   **`trunk`**: Trunking.

   **`NAME`**: Trunk name. It must have the format **`tX`**, where **`X`** represents any number in the range **`1-7`**.

   **`PORTS-GROUP`**: Group of ports to be *trunked*. Any number of ports may be selected.

   <u>Example</u>

   ```
   OS900(config)# port trunk t2 2,4
   OS900(config)#
   ```

3. Optionally, in order to provide traffic load balancing, select a hash function appropriate to the layer at which datagrams are transferred through the trunk using the command:

   **`port trunk mode l2|l3|l4|port`**

   where,

   **`l2`**: Hashing based on source/destination MAC address.

   **`l3`**: Hashing based on source/destination IP address.

   **`l4`**: Hashing based on TCP/UDP port.

   **`port`**: Hashing based on physical port or trunk.

Example

```
OS900(config)# port trunk mode l2
OS900(config)#
```

4. Optionally, in order to set the time the LACP mechanism is to wait before it breaks the link between two ports of a trunk in the event that either of the ports does not receive an LACP integrity packet, invoke the command:

   **lacp timers timeout <3-60>**

   where,

   **<3-60>**: Timeout time in seconds. Default: 3 seconds.

Example

```
OS900(config)# lacp timers timeout 7
OS900(config)#
```

To reset the timeout time to the default value (3 seconds), invoke the command:

**no lacp timers timeout**

# Activation

LACP can be activated on a port trunk or on a group of untrunked ports.

## Trunk

### LACP

#### *Active Mode*

To activate LACP on a port *trunk* and to set the port trunk to operate in *active mode*[30], invoke the command:

**port trunk NAME lacp**

where,

**NAME**: Trunk name. It must have the format **tX**, where **X** represents any number in the range **1-7**.

**lacp**: Enable LACP.

Example

```
OS900(config)# port trunk t2 lacp
OS900(config)#
```

#### *Passive Mode*

To activate LACP on a port *trunk* and to set the port trunk to operate in *passive mode*[31], invoke the command:

**port trunk NAME lacp passive**

where,

**NAME**: Trunk name. It must have the format **tX**, where **X** represents any number in the range **1-7**.

**lacp**: Enable LACP.

**passive**: Passive mode for LACP.

Example

```
OS900(config)# port trunk t2 lacp passive
OS900(config)#
```

### Rapid LACP

To activate Rapid LACP (reduced-time-session-establishment LACP) on a port *trunk* and to set the port trunk to operate in *active mode*, invoke the command:

**port trunk NAME rapid-lacp**

[30] In active mode, the OS900 initiates LACP packets.

[31] In passive mode, the OS900 does not initiate LACP packets. However, it can respond to received LACP packets.

where,

**NAME**: Trunk name. It must have the format **tX**, where **X** represents any number in the range **1-7**.

**rapid-lacp**: Enable Rapid LACP.

Example

```
OS910(config)# port trunk t1 rapid-lacp
OS910(config)#
```

# Port

## LACP

### *Active Mode*

To activate LACP on one or more *ports* and to set the ports to operate in *active mode*, invoke the command:

**port lacp (PORTS-GROUP|all)**

where,

**lacp**: Enable LACP.

**PORTS-GROUP**: Group of ports to participate in LACP.

**all**: All ports to participate in LACP.

Example

```
OS910(config)# port lacp 1-3
OS910(config)#
```

### *Passive Mode*

To activate LACP on one or more *ports* and to set the *ports* to operate in *passive mode*, invoke the command:

**port lacp passive (PORTS-GROUP|all)**

where,

**passive**: Passive mode for LACP.

**PORTS-GROUP**: Group of ports to participate in LACP.

**all**: All ports to participate in LACP.

Example

```
OS910(config)# port lacp passive 2-4
OS910(config)#
```

## Rapid LACP

To activate Rapid LACP (reduced-time-session-establishment LACP) on one or more *ports* and to set the ports to operate in *active mode*, invoke the command:

**port rapid-lacp (PORTS-GROUP|all)**

where,

**rapid-lacp**: Enable Rapid LACP.

**PORTS-GROUP**: Group of ports to participate in Rapid LACP.

**all**: All ports to participate in Rapid LACP.

Example

```
OS910(config)# port rapid-lacp 1,4
OS910(config)#
```

# Deactivation

## Trunk

### LACP

To deactivate LACP on a port *trunk*, invoke the command:

**`no port trunk NAME lacp`**

where,

**`NAME`**: Trunk name. It must have the format **`tX`**, where **`X`** represents any number in the range **`1-7`**.

Example

```
OS910(config)# no port trunk t1 lacp
OS910(config)#
```

### Rapid LACP

To deactivate Rapid LACP on a port *trunk*, invoke the command:

**`no port trunk NAME rapid-lacp`**

where,

**`NAME`**: Trunk name. It must have the format **`tX`**, where **`X`** represents any number in the range **`1-7`**.

Example

```
OS910(config)# no port trunk t1 rapid-lacp
OS910(config)#
```

## Port

To deactivate LACP or Rapid LACP on one or more *ports*, invoke the command:

**`no port lacp PORTS-GROUP|all`**

where,

**`PORTS-GROUP`**: Group of ports to participate in LACP.

**`all`**: All ports to participate in LACP.

Example

```
OS910(config)# no port lacp 1,4
OS910(config)#
```

# Viewing

## Port Trunk Configuration

To view the port trunk LACP configuration:

1. Enter **`enable`** mode.
2. Invoke the following command:

   **`show port trunk [NAME]`**

   where,

   **`show`**: Display.

   **`port`**: Port action.

   **`trunk`**: Trunking.

   **`[NAME]`**: (optional) ID of trunk, e.g., **`t1`**. If no value is entered for this argument, all Port Trunks will be shown.

Example

```
OS900# show port trunk t2
Trunk Mode: L3
```

```
NAME     PORTS                            LINKED-PORTS
-------------------------------------------------------------
t2       2,4

OS900#
```

### Port Configuration

To view the port LACP configuration:

1. Enter **enable** mode.
2. Invoke the following command:
   **show port lacp**

Example

```
OS900# show port lacp
LACP INFO
=========
System Id: 00:0F:BD:00:36:67
System Priority: 32768
PORT  LACP      MODE     KEY    TRUNK   PARTNER   STATE
--------------------------------------------------------
1     disable
2     enable    active   auto   t2       0         disable
3     enable    active   auto   t2       0         disable
4    enable    active   auto   t2       0         disable
OS900#
```

## Deleting

To delete a port *trunk*:

1. Enter **configure terminal** mode.
2. Invoke the following command:
   **no port trunk NAME**
   where,
   **no**: Negation.
   **port**: Port action.
   **trunk**: Trunking.
   **NAME**: Trunk name. It must have the format **tX**, where **X** represents any number in the range **1-7**.

Example

```
OS900(config)# no port trunk t6
OS900(config)#
```

## Adding/Deleting Ports to a Trunk

The procedure essentially consists of deleting the Port Trunk and reconfiguring it with the new set of ports.

To add or delete ports to an existing Port Trunk:

1. Enter the mode of each interface that has the Port Trunk as member and delete the Port Trunk using the command:
   **ports del PORTS-GROUP**
   where,
   **PORTS-GROUP**: Port Trunk to be deleted (e.g., **t1**)
2. If the Port Trunk is tagged[32], enter **configure terminal** mode and set it in untagged mode by and invoking the command:

[32] Tagged mode is required if a port is a member of two or more VLANs.

**`port tag-outbound-mode untagged PORTS-GROUP`**

where,

**`PORTS-GROUP`**: Port Trunk to be untagged (e.g., **`t1`**)

3. If the Port Trunk is set in LACP mode, delete the Port Trunk using the command:

   **`no port trunk NAME lacp|rapid-lacp`**

   where,

   **`NAME`**: Name of Port Trunk to be deleted (e.g., **`t1`**)

4. Delete the Port Trunk using the command:

   **`no port trunk NAME`**

   where,

   **`NAME`**: Name of Port Trunk to be deleted (e.g., **`t1`**)

5. Reconfigure the Port Trunk using the command:

   **`port trunk NAME PORTS-GROUP`**

   where,

   **`NAME`**: Name of Port Trunk (e.g., **`t1`**)

   **`PORTS-GROUP`**: Ports to be members of the Port Trunk

6. If required, set the Port Trunk in tagged mode using the command:

   **`port tag-outbound-mode tagged PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Port Trunk to be tagged

7. Include the reconfigured Port Trunk (e.g., **`t1`**) in the respective interfaces using the command:

   **`ports add PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Port Trunk to be added (e.g., **`t1`**)

# Chapter 14: Quality of Service (QoS)

## DiffServ Service Levels

A Diffserv Service Level (SL) is a priority with which a packet (or frame) is serviced. The user can set the classification criteria for *ingress* packets and then assign an SL (number between 1 and 8) to each class. SL = 8 is highest service priority. SL = 1 is lowest service priority.

An ingress packet is directed to the associated one of eight hardware egress queues of a port according to the SL assigned to the ingress packet.

SLs are used only internally by the OS900.

SL assignments can be subsequently overridden by new ones by an ACL – for details refer to ***Chapter 15:*** *Extended Access Lists* (ACLs), page *295*.

The user can also set the OS900 to mark (change) the VPT and DSCP values to new ones for *egress* packets as described in the section *Marking*, page *285*.

## Assigning SLs

### CPU Ingress Packets

#### Default

The default SLs assigned to ingress packet types/protocols to be transmitted from the CPU are shown in *Table 10*, below.

**Table 10: Default Protocol-to-SL Map**

| Protocol | SL |
|---|---|
| OSPF or RIP | 7 |
| VRRP | 6 |
| ISIS | 7 |
| ARP | 7 |
| ICMP | 7 |
| Other | By ToS |

#### Custom

To assign any SL value to an ingress packet type/protocol to be transmitted from the CPU, invoke the command:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`cpu-traffic-sl transmit (ospf-rip|vrrp|isis|arp|icmp|data) <1-8>`**
   where,
   **`ospf-rip`**: OSPF or RIP
   **`vrrp`**: VRRP
   **`isis`**: IS-IS
   **`arp`**: ARP
   **`icmp`**: ICMP
   **`data`**: Other
   **`<1-8>`**: Range of SLs from which one is to be selected for mapping to a packet type/protocol.

Example

```
OS904(config)# cpu-traffic-sl transmit vrrp 3
OS904(config)#
```

To reassign the default values to the packet types/protocols to be transmitted from the CPU, invoke the command: **`no cpu-traffic-sl transmit (ospf-rip|vrrp|isis|arp|icmp|data)`**

### Viewing

To view the protocol-to-SL map for ingress packet types/protocols to be transmitted from the CPU:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show cpu-traffic-sl`**

Example

```
OS904# show cpu-traffic-sl
CPU Traffic Type  :  Transmit Service Level
============================================
OSPF / RIP        :           7
VRRP              :           6
ISIS              :           7
ARP               :           7
ICMP              :           7
Other Data        :         By TOS
OS904#
```

## Non-CPU Ingress Packets

The user can assign SLs to ingress packet types/protocols on the basis of any of the following: Port number, VPT, DSCP, or ACL mark SL action. If the user does not assign an SL, ingress packets without a VPT or DSCP, or without an ACL mark SL action for their ports of entry, are assigned the SL value 1. The OS900 maps VPTs to SLs according to *Table 11*, page *283*, and DSCPs to SLs according to *Table 12*, page *284*. An ACL rule action can be used to assign SLs as described in the section *Stage 2 – Actions on Packet*, page *304*.

# Selecting an SL Criterion

Several SLs may apply to a class of ingress packets. To dictate the criterion to be used for selecting the SL for the ingress packet class, do the following:

1. Enter **`configure terminal`** mode.
2. Select a trust mode (**`l2`**, **`l2l3`**, **`l3`**, or **`port`** – described below) by invoking the following command:
   **`port qos-trust PORTS-GROUP|all l2|l2l3|l3|port`**
   where,
   **`PORTS-GROUP`**: Group of ports. (Trunk ports may be included in the group.)
   **`all`**: All ports.
   **`l2`**: Layer 2 VPT bits to be used to assign an SL to a packet. (Default)
   **`l2l3`**: Layer 3 DSCP bits to be used to assign an SL to a packet, otherwise use Layer 2 VPT bits to assign an SL.
   **`l3`**: Layer 3 DSCP bits to be used to assign an SL to a packet.
   **`port`**: Default priority (SL) of the ingress port to be used to assign an SL to a packet.

**Note**
If an ACL is bound to a port, the criterion for selecting the SL as specified in the ACL overrides all the trust modes!

# Ingress-Port-to-SL Map

To enable the OS900 to map SLs to *ingress* packets according to their port of entry:

1. Enter **`configure terminal`** mode.
2. Invoke the following command:
   **`port sl <1-8> PORTS-GROUP|all`**
   where,
   **`port`**: Port action.
   **`sl`**: SL.
   **`<1-8>`**: (Port priority) Range of SLs from which one is to be selected. (Default: **`1`**.)
   **`PORTS-GROUP`**: Group of ports to which the SL is to be assigned.
   **`all`**: All ports

Example

```
OS900(config)# port sl 7 2-4
port 2 priority set to: 7
port 3 priority set to: 7
port 4 priority set to: 7
OS900(config)#
```

# Original-VPT-to-SL Map

The Original-VPT-to-SL Map is used by the OS900 to assign an SL to an *ingress* packet according to its VPT.

## Default

The default Original-VPT-to-SL Map is shown in *Table 11*, below.

**Table 11: Default Original-VPT-to-SL Map**

| Original VPT | SL |
|---|---|
| 0 | 1 |
| 1 | 2 |
| 2 | 3 |
| 3 | 4 |
| 4 | 5 |
| 5 | 6 |
| 6 | 7 |
| 7 | 8 |

## Custom

The user can change the default Original-VPT-to-SL Map as follows:

1. Enter **`configure terminal`** mode.
2. Invoke the following command:
   **`diffserv orig-vpt RANGE sl <1-8>|default`**
   where,
   **`diffserv`**: Differentiated Services.
   **`orig-vpt`**: VPT value of ingress packet.
   **`RANGE`**: Range of VPT values to be mapped to an SL. Any one or more VPT values 0-7 can be selected.
   **`sl`**: SL.
   **`<1-8>`**: Range of SLs from which one is to be selected.

**default**: Default SL for the VPT value. (*Table 11*, above, shows the default SL for each VPT value.)

To revoke the above command, invoke the command:

**no diffserv orig-vpt RANGE**

Example

```
OS900(config)# diffserv orig-vpt 0-3 sl 8
OS900(config)# diffserv orig-vpt 4-7 sl 1
OS900(config)#
```

### Viewing

To view the Original-VPT-to-SL Map, invoke the **enable** mode command **show diffserv**.

Example

```
OS900(config)# do show diffserv

VPT Classification & Marking Table
==================================
orig-vpt service-level mark-vpt
==================================
4-7       1             0
          2             1
          3             2
          4             3
          5             4
          6             5
          7             6
0-3       8             7
OS900(config)#
```

## Original-DSCP-to-SL Map

The Original-DSCP-to-SL Map is used by the OS900 to assign an SL to an *ingress* packet according to its DSCP.

### Default

The default Original-DSCP-to-SL Map is shown in *Table 12*, below.

**Table 12: Default Original-DSCP-to-SL Map**

| Original DSCP | SL |
|---|---|
| 0-9,11-17,19,21,23-25,27,29,31-33,35,37,39-45,47-63 | 1 |
| 10 | 2 |
| 20,22 | 3 |
| 18 | 4 |
| 28,30 | 5 |
| 26 | 6 |
| 36,38 | 7 |
| 34,46 | 8 |

### Custom

The user can change the default Original-DSCP-to-SL Map as follows:

1. Enter **configure terminal** mode.
2. Invoke the following command:

   **diffserv orig-dscp RANGE sl <1-8>|default**

   where,

**`diffserv`**: Differentiated Services.

**`orig-dscp`**: DSCP value of ingress packet.

**`RANGE`**: Range of DSCP values to be mapped to an SL. Any one or more DSCP values 0-63 can be selected.

**`sl`**: SL.

**`<1-8>`**: Range of SLs from which one is to be selected.

**`default`**: Default SL for the DSCP value. (*Table 12*, page *284*, shows the default SL for each DSCP value.)

To revoke the above command, invoke the command:

**`no diffserv orig-dscp RANGE`**

Example

```
OS910(config)# diffserv orig-dscp 4-7,19 sl 3
OS910(config)#
```

### View

To view the Original DSCP to SL Map, invoke the command **`do show diffserv`**.

Example

```
OS910(config)# do show diffserv

DSCP Classification & Marking Table
===================================
orig-dscp                                             service-level mark-dscp
============================================================================
0-3,8-9,11-17,20-25,27,29,31-33,35,37,39-45,47,49-63        1         12
10                                                          2         10
4-7,19                                                      3         20
18                                                          4         18
28,30                                                       5         28
26                                                          6         26
36,38                                                       7         36
34,46,48                                                    8         34
```

Notice that as a result of the mapping, DSCP values 20 and 22 that map to SL3 in the default map are transferred to SL1.

# Marking

## General

The OS900 can be set to mark *egress* packets with a new VPT and/or DSCP according to the SL of the packet using a global[33] map (*Table 13* or *Table 14*; both user-configurable) or with an ACL rule action (as described in the section *Stage 2 – Actions on Packet*, page *304*). The global map *only defines* the values that will be used when marking is activated. In order to *activate* marking, the user has to set the ingress port to do so. (The ingress port *turns on* marking for each packet, but the actual marking is done on the egress port.) Both the mark mode (e.g., VPT, or DSCP, or etc.) and mark value (e.g., 1, or 2, or etc.) are set in the ACL rule.

Packets to be transmitted from the CPU have SLs – see section *CPU Ingress Packets*, page *281*. These packets are marked with VPTs according to *Table 13*.

## SL-to-New-VPT Map

The SL-to-New-VPT Map is used to assign a VPT to an *egress* packet according to its SL.

### Default

The default SL-to-New-VPT Map is shown in *Table 13*, below.

[33] Applicable to all ports of the OS900.

**Table 13: Default SL-to-New-VPT Map**

| SL | Mark (New) VPT |
|---|---|
| 1 | 0 |
| 2 | 1 |
| 3 | 2 |
| 4 | 3 |
| 5 | 4 |
| 6 | 5 |
| 7 | 6 |
| 8 | 7 |

**Custom**

The user can change the default SL-to-New-VPT Map as follows:

1. Enter **`configure terminal`** mode.
2. Invoke the following command:

   **`diffserv sl <1-8>|all mark-vpt default|<0-7>`**

   where,

   **`diffserv`**: Differentiated Services.

   **`sl`**: SL.

   **`<1-8>`**: Range of SLs from which one is to be selected for mapping to a VPT value.

   **`all`**: All eight SLs.

   **`mark-vpt`**: VPT value to be changed.

   **`default`**: Default VPT value for the SL. (*Table 13*, above, shows the default VPT value for each SL.)

   **`<0-7>`**: Range of VPT values from which one is to be selected.

   To revoke the above command, invoke the command:

   **`no diffserv sl <1-8>|all mark-vpt`**

Example

```
OS900(config)# diffserv sl all mark-vpt 5
OS900(config)#
```

The values in the **Mark (New) VPT** column can be changed again with the command **`action mark sl <1-8> vpt <0-7>`** under **`rule`** mode under **`access-list`** mode under **`configure terminal`** mode.

**View**

To view the SL-to-New-VPT Map, invoke the command **`do show diffserv`**[34].

Example

```
OS900(config)# do show diffserv

VPT Classification & Marking Table
==================================
orig-vpt service-level mark-vpt
==================================
0         1              5
1         2              5
2         3              5
3         4              5
```

[34] It will be recalled that any command in **`enable`** mode can be accessed from any mode by prefixing the command **`do`**.

```
4          5              5
5          6              5
6          7              5
7          8              5
OS900(config)#
```

## SL-to-New-DSCP Map

The SL-to-New-DSCP Map is used to assign a DSCP to an *egress* packet according to its SL.

### Default

The default SL-to-New-DSCP Map is shown in *Table 14*, below.

**Table 14: Default SL-to-New-DSCP Map**

| SL | Mark (New) DSCP |
|---|---|
| 1 | 12 |
| 2 | 10 |
| 3 | 20 |
| 4 | 18 |
| 5 | 28 |
| 6 | 26 |
| 7 | 36 |
| 8 | 34 |

### Custom

The user can change the default SL-to-New-DSCP Map as follows:

1. Enter **`configure terminal`** mode.
2. Invoke the following command:

    **`diffserv sl <1-8>|all mark-dscp <0-63>|default`**

    where,

    **`diffserv`**: Differentiated Services.

    **`sl`**: SL.

    **`<1-8>`**: Range of SLs from which one is to be selected.

    **`all`**: All eight SLs.

    **`mark-dscp`**: New DSCP value(s) for ingress packet.

    **`<0-63>`**: Range of DSCP values to be mapped to an SL. Any one of the DSCP values 0-63 can be selected.

    **`default`**: Default DSCP value for the SL. (*Table 14*, page *287*, shows the default DSCP value for each SL.)

    To revoke the above command, invoke the command:

    **`no diffserv sl <1-8>|all mark-dscp`**

Example

```
OS910(config)# diffserv sl 7 mark-dscp 0
OS910(config)#
```

The values in the **Mark (New) DSCP** column can be changed again with the command **`action mark sl <1-8> dscp <0-63>`** under **`rule`** mode under **`access-list`** mode under **`configure terminal`** mode .

### View

To view the SL-to-New-DSCP Map, invoke the command **`do show diffserv`**.

Example

```
OS910(config)# do show diffserv
DSCP Marking Table
==================
orig-dscp                                                       service-level mark-dscp
============================================================================
0-3,8-9,11-17,20-25,27,29,31-33,35,37,39-45,47-63               1             12
10                                                              2             10
4-7,19                                                          3             20
18                                                              4             18
28,30                                                           5             28
26                                                              6             26
36,38                                                           7             0
34,46                                                           8             34
```

## Activation

To activate marking:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port qos-marking PORTS-GROUP|all dscp|vpt|vptdscp**

   where,

   **PORTS-GROUP**: Group of ports. (Trunk ports may be included in the group.)
   **all**: All ports.
   **dscp**: Mark DSCP bits according to the SL of a packet.
   **vpt**: Mark VPT bits according to the SL of a packet.
   **vptdscp**: Mark Layer 3 DSCP bits and Layer 2 VPT bits according to the SL of a packet.

# Examples

## VPT

This example is provided to demonstrate the procedure for setting up the OS900 to direct ingress packets at a specific port that have a specific VPT to an egress queue having a specific SL and to mark these packets with a different VPT at egress.

Suppose it is required:

- To direct ingress packets at Port 1
- That have VPT 5
- To the egress queue having SL 6
- And to mark these packets with VPT 4 at egress

The sequence of CLI commands to be invoked to implement the requirement is shown below.

```
----Modification of Table 11, page 283, so that the same SL is assigned to the VPT at ingress and to that required at egress----
OS900(config)# diffserv orig-vpt 5,4 sl 6

--------------------Modification of Table 13, page 286, so that the required VPT at egress is assigned to required SL--------------------
OS900(config)# diffserv sl 6 mark-vpt 4

------------------------Identification of the port at which ingress packets are to be queued according to their VPT------------------------
OS900(config)# port qos-trust 1 l2

---------------------------------------------Activation of marking for the selected port and VPT value---------------------------------------------
OS900(config)# port qos-marking 1 vpt
```

In the above example, since Port 1 is a dual port[35], both the ingress and the egress VPT are specified in the command **`diffserv orig-vpt 5,4 sl 6`**.

*Figure 36*, below, shows the stages at which a packet passing through the OS900 ports is:

– assigned an SL for placement in an egress queue, and
– marked with the VPT required for egress.

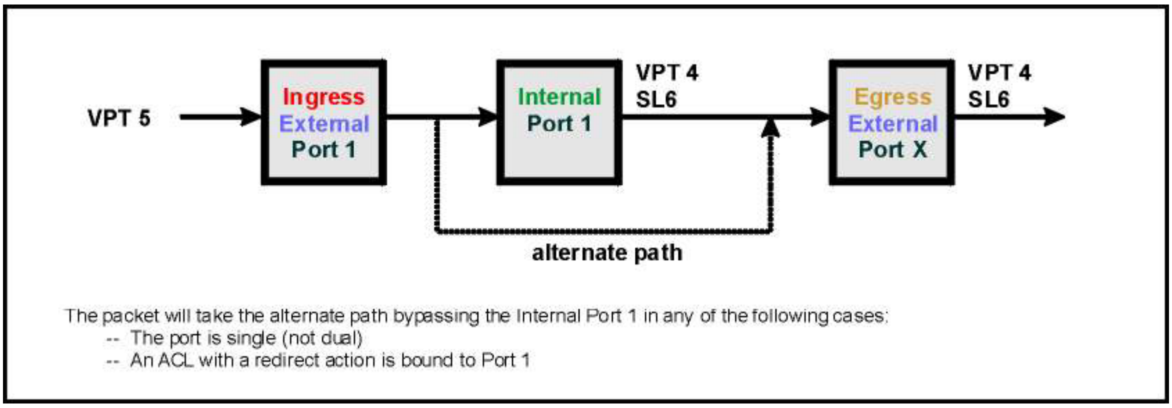



**Figure 36: SL Assignment & VPT Marking of a Packet**

## DSCP

This example is provided to demonstrate the procedure for setting up the OS900 to direct ingress packets at a specific port that have a specific DSCP to an egress queue having a specific SL and to mark these packets with a different DSCP at egress.

Suppose it is required:

– To direct ingress packets at Port 1
– That have DSCP 10
– To the egress queue having SL 6
– And to mark these packets with DSCP 18 at egress

The sequence of CLI commands to be invoked to implement the requirement is shown below.

```
----Modification of Table 12, page 284, so that the same SL is assigned to the DSCP at ingress and to that required at egress----
OS910(config)# diffserv orig-dscp 10,18 sl 6

--------------------Modification of Table 14, page 287, so that the required DSCP at egress is assigned to required SL--------------------
OS910(config)# diffserv sl 6 mark-dscp 18

------------------------Identification of the port at which ingress packets are to be queued according to their DSCP------------------------
OS910(config)# port qos-trust 1 l3

---------------------------------------------Activation of marking for the selected port and DSCP value---------------------------------------------
OS910(config)# port qos-marking 1 dscp
```

In the above example, since Port 1 is a dual port, both the ingress and the egress DSCP are specified in the command **`diffserv orig-dscp 10,18 sl 6`**.

*Figure 37*, below, shows the stages at which a packet passing through the OS900 ports is:

– assigned an SL for placement in an egress queue, and
– marked with the DSCP required for egress.

[35] Dual ports are described in the section *Regular, Dual, and Extra Internal* Ports, page *155*.

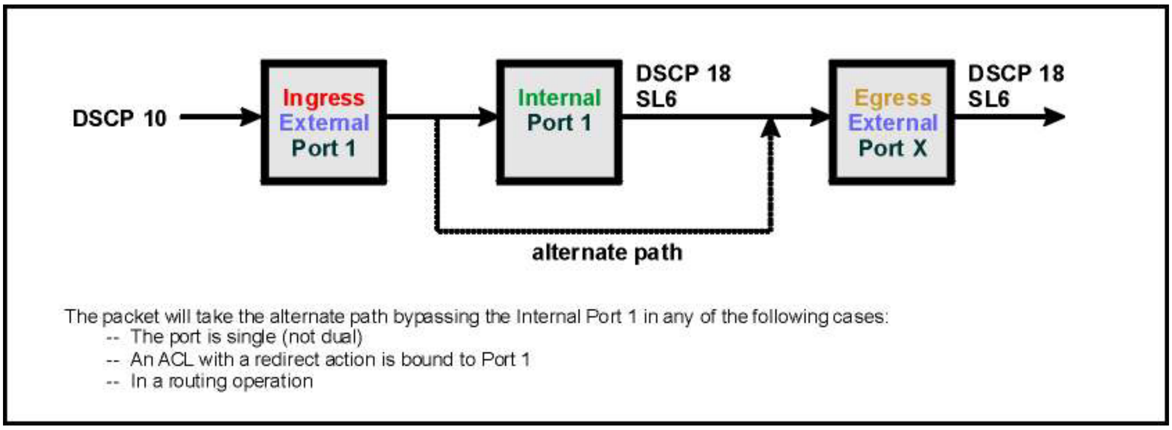



**Figure 37: SL Assignment & DSCP Marking of a Packet**

# Statistics

## General

This section describes how to enable statistics gathering per-port per-SL while preserving the mapping function DSCP → SL, VPT → SL.

The OS900 can be configured to collect up to sixteen sets of counts (since there are sixteen statistics counters). The readings of the counts are displayed in tabular format. The entry `NA` means not applicable.

## Configuration

1. Two new global tables can be configured. The first one maps VPT to SL, the second maps DSCP to SL.

   To configure the VPT → SL global table:

   1.1. Enter **`configure terminal`** mode.

   1.2. Enter VPT-to-SL mode by invoking the command:
   **`sl-stat-table-vpt`**

   1.3. Invoke the command:
   **`orig-vpt <0-7> sl <1-8> [vpt <0-7>]`**
   where,
   **`<0-7>`**: Range of VPT values of ingress packets from which one value is to be selected.
   **`<1-8>`**: Range of SLs from which one is to be assigned to ingress packets having the VPT value selected just above.
   **`[vpt <0-7>]`**: The VPT value to replace that of ingress packets having the value selected above.

   To exclude packets with a certain VPT from the 'VPT-to-SL' global table, i.e., to exclude such packets from being included in the statistics, invoke the command:
   **`no orig-vpt <0-7>`**
   where,
   **`<0-7>`**: Range of VPT values of ingress packets to be excluded.

   To configure the DSCP → SL global table:

   1.4. Exit to **`configure terminal`** mode.

   1.5. Enter DSCP-to-SL mode by invoking the command:
   **`sl-stat-table-tos`**

   1.6. Invoke the command:
   **`orig-tos TOS_HEX_VALUE TOS_HEX_MASK sl <1-8>`**
   where,

**TOS_HEX_VALUE**: ToS value (*hexadecimal* number selectable from the range **0** to **FF**)

**TOS_HEX_MASK**: ToS mask (*hexadecimal* number selectable from the range **0** to **FF**)

**<1-8>**: SL value (selectable from the range **1** to **8**)

To exclude packets with a certain DSCP from the 'DSCP-to-SL' global table, i.e., to exclude such packets from being included in the statistics, invoke the command:

**no orig-tos DSCP_HEX_VALUE DSCP_HEX_MASK**

where,

**<0-7>**: Range of VPT values of ingress packets to be excluded.

2. Enable accounting for one or more ports specifying whether the classification is by VPT and/or DSCP by invoking either of the following commands:

   **port sl-account dscp PORTS-GROUP [vpt PORTS-GROUP]**

   **port sl-account vpt PORTS-GROUP [dscp PORTS-GROUP]**

   where,

   **PORTS-GROUP**: (First appearance) Group 1 of ports[36].

   **PORTS-GROUP**: (Second appearance) Group 2 of ports. Each port in this group must be different from any port in Group 1 because *only one* ACL may be bound to a port!

   (To drop such packets, invoke the command **no port sl-account dscp PORTS-GROUP [vpt PORTS-GROUP]** or **no port sl-account vpt PORTS-GROUP [dscp PORTS-GROUP]**.)

3. By default, the global policy for automatic (system-generated) ACLs (e.g., for accounting) is deny (drop) packets that do not strictly meet the user specifications for the packets. To allow (forward) such packets, invoke either of the following commands:

   **port sl-account default policy permit dscp PORTS-GROUP [vpt PORTS-GROUP]**

   **port sl-account default policy permit vpt PORTS-GROUP [dscp PORTS-GROUP]**

   where,

   **PORTS-GROUP**: (First appearance) Group 1 of ports.

   **PORTS-GROUP**: (Second appearance) Group 2 of ports. Each port in this group must be different from any port in Group 1 because *only one* ACL may be bound to a port!

   (To drop such packets, invoke the command **no port sl-account default policy permit dscp PORTS-GROUP [vpt PORTS-GROUP]** or **no port sl-account default policy permit vpt PORTS-GROUP [dscp PORTS-GROUP]**.)

## Viewing

To view the statistics counters:

1. Enter **enable** mode.
2. Invoke the command:

   **show sl-stat-counters (PORTS-GROUP|all) sl (SL-GROUP|all)**

   where,

   **PORTS-GROUP**: Group of ports.

   **all**: (First appearance) All ports.

   **SL-GROUP**: Group of SLs.

   **all**: (Second appearance) All SLs.

To view the statistics counters *with refresh* (continual data update):

1. Enter **enable** mode.

[36] Each and every port in the group must NOT have a user-defined ACL bound to it.

2. Invoke the command:
   **`monitor sl-stat-counters (PORTS-GROUP|all) sl (SL-GROUP|all)`**
   where,
   `PORTS-GROUP`: Group of ports.
   `all`: (First appearance) All ports.
   `SL-GROUP`: Group of SLs.
   `all`: (Second appearance) All SLs.

### Clearing

To clear the statistics counters:

**`clear sl-stat-counters (PORTS-GROUP|all) sl (<1-8>|all)`**

where,

`PORTS-GROUP`: Group of ports.

`all`: (First appearance) All ports.

`<1-8>`: Group of SLs.

`all`: (Second appearance) All SLs.

# Hierarchical QoS

### General

Certain models of the OS900 have extra internal ports, one or more of which can be flexibly assigned to a regular port, dual port, or trunk. Such ports are described in the section *Regular, Dual, and Extra Internal* Ports, page *155*. Trunks are described in ***Chapter 13:*** *IEEE 802.3ad Link Aggregation (LACP)*, page *273*.

This section shows how extra internal ports can be used to provide ingress shaping of traffic entering a regular port, dual port, or trunk on a per-VLAN tag basis.

An extra internal port may be assigned to one and only one regular port, dual port, or trunk.

### Principle of Operation

Traffic of several VLANs entering a specific port are separated into streams, each containing frames of one and the same VLAN. This separation is achieved by redirecting the frames into the internal port (if the ingress port is a dual port) and extra internal ports so that only frames of the same VLAN enter these ports. Each stream is then subjected to ingress shaping after which the streams are combined and transmitted on a common egress port/trunk.

### Example

#### Purpose

This example is used to show how to configure an OS900 so that it performs ingress shaping of traffic (entering a dual port and exiting a regular or dual port) on a per-VLAN tag basis.

### Network

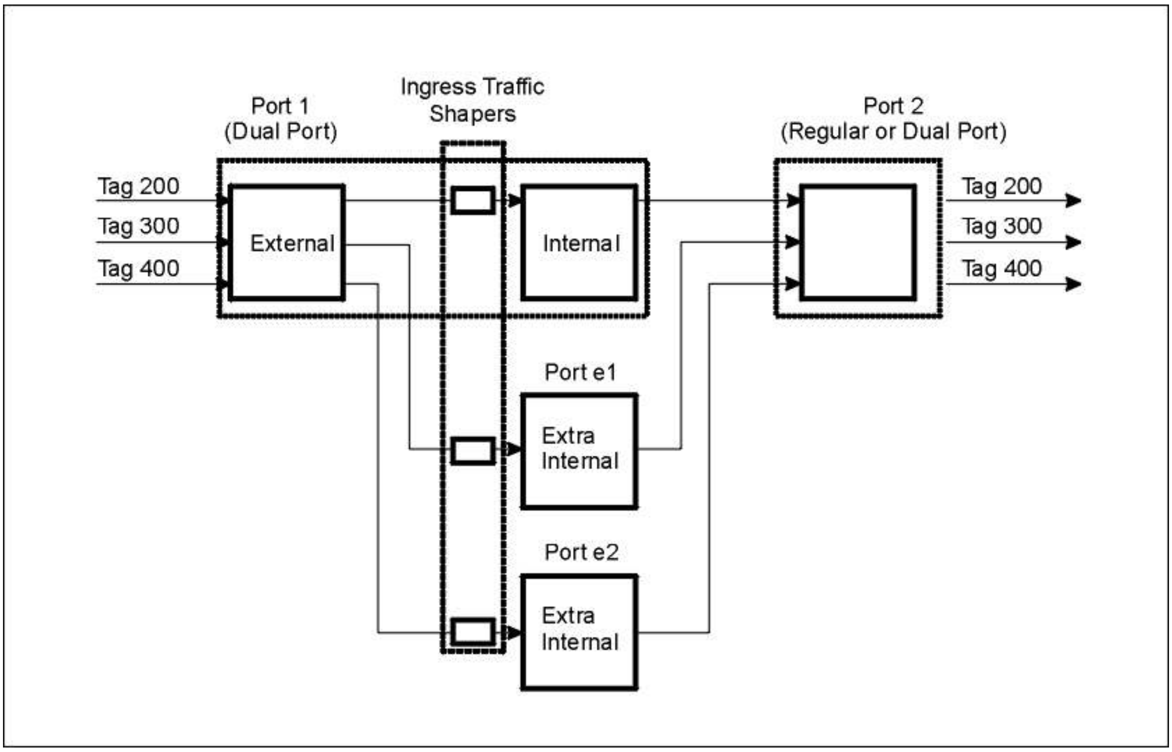



**Figure 38: Ingress Traffic Shaping using Hierarchical QoS**

### Configuration

```
-----------------------------------Creating Inband VLAN Interfaces for Traffic Streams-----------------------------------

interface vlan vif200
 tag 200
 ports 1-2
!
interface vlan vif300
 tag 300
 ports 1-2
!
interface vlan vif400
 tag 400
 ports 1-2
!

---------------------------------------------Enabling Use of Extra Internal Ports---------------------------------------------

!
port extra e1-e2
!

-------------------------Creating an Access List for Redirecting Traffic on a per-VLAN Basis-------------------------

access-list extended acl1
 rule 10
  tag eq 200
  action permit
rule 20
  tag eq 300
  action redirect port e1
rule 30
  tag eq 400
  action redirect port e2
!
```

```
-------------------------------------------------------Ingress Shaping Setting-------------------------------------------------------

port ingress-shaping rate 150m burst-size 20k e1
port ingress-shaping rate 120m burst-size 20k e2
!
port acl-binding-mode by-port 1
port access-group acl1 1
!
```

# Chapter 15: Extended Access Lists (ACLs)

This chapter shows how to create and apply extended Access Lists (ACLs) for handling ingress and egress traffic.

## Definition

An ACL is a set of rules for handling traffic at each OS900 port or VLAN interface. Each rule consists of a set of packet *attribute values* (for the purpose of packet classification) and *actions* to be performed on packets that have these values.

Examples of attributes are: Protocol, Source IP address, Destination IP address, Source port, Destination port, VLAN tag, etc.

Examples of actions are: Drop packet, Forward packet, Mark an SL, Mirror packet to CPU, Handle packets according to an Action List, etc.

## Applicability

An ACL can be applied to one or more:

- VLAN interfaces
- *Specific* ports (even if the ports are members of different VLAN interfaces)

The advantage in applying one ACL to several ports/interfaces (i.e., using the ACL in sharing mode) becomes evident when the ACL has to be modified. In such an instance the ACL needs to be modified *just once* rather than several times, once for each port/interface.

Also, two ACLs can be created specifying two traffic conditioners to provide dual leaky-bucket policing of traffic. The procedure is described in the section *Dual Leaky-Bucket Policer*, page *367*.

## Number

Up to 1K ACLs can be bound to ports and VLAN interfaces.

## Global Profiles

### General

A global profile is a policy for *all* ACLs (whether existing or to be configured in the future) in handling *ingress* packets according to their tags.

### Types

There are three global profiles:

- *Normal*
- *Doubletag*
- *MPLS EXP*

One of these three profiles is mandatorily assigned to *all* ACLs. The normal global profile is the *default*.

***Normal***

This profile is used for handling *single*-tag packets. If **`normal`** profile is selected:

The classifications[37] **`ctag`** and **`c-vpt`** are illegal classifications. If they are used, binding of the ACL will fail!

The classifications **`tag`** and **`vpt`** apply to the *first* tag of the ingress traffic, *before* addition of a tag to packets according to the port's outbound tag mode[38].

***Doubletag***

This profile is used for handling *double*-tag packets. If **`double-tag`** profile is selected:

The classifications **`ctag`** and **`c-vpt`** apply to the *second* tag of the ingress traffic, *before* handling of packets according to the port's outbound tag mode.

The classifications **`tag`** and **`vpt`** apply to the *first* tag of the ingress traffic, *after* handling of packets according to the port's outbound tag mode.

***MPLS EXP***

This profile is used for handling *MPLS* packets with EXP bits.

## Selection

The user can select the profile to be assigned to all ACLs as follows:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`access-list extended-profile normal|double-tag|mpls-exp`**

   where,

   **`normal`**: Single-tag packets

   **`double-tag`**: Double-tag packets

   **`mpls-exp`**: MPLS packets with EXP bits

## Changing

To change the profile selected to be assigned to all ACLs:

1. First make sure that all ACLs are unbound (as described in the section *Unbinding*, page *318*.
2. Invoke the command:

   **`access-list extended-profile normal|double-tag|mpls-exp`**

   where,

   **`normal`**: Single-tag packets

   **`double-tag`**: Double-tag packets

   **`mpls-exp`**: MPLS EXP-bits packets

## Default

To select the default profile (*Normal*) for all ACLs:

1. Enter **`configure terminal`** mode.
2. Invoke either of the following commands:

   **`default access-list extended-profile`**

   Or

   **`access-list extended-profile normal`**

# Creating/Accessing

To create or access an ACL:

1. Enter **`configure terminal`** mode

[37] Selectable in **`rule`** mode, and detailed in the section *Stage 1 – Packet Classification*, page *297*.

[38] If the mode is **`q-in-q`** or **`untagged`**, a VLAN tag is added. If the mode is **`hybrid`**, a VLAN tag is added to untagged packets. For details on these modes, refer to the section *Outbound Tag Mode*, page *137*.

2. Invoke the command:
   **`access-list extended WORD`**
   where,
   **`WORD`**: Name of the ACL (new or existing)

| | |
|---|---|
| | **Note**<br>If an ACL already exists, it is enough to type the first few characters unique to its name and press Tab in order to access the ACL or complete its name. |

<u>Example</u>

```
OS900> enable
OS900# configure terminal
OS900(config)# access-list extended ACL1
OS900(config-access-list)#
```

The ACL name (**`ACL1`** in the example above) becomes the instance (current) and the CLI enters ACL mode (as indicated by the prompt '`OS900(config-access-list)#`').

If this ACL has just been created, it is empty. To make it useful, rules have to be created for it. To create, display, edit, move, and delete rules, refer to the section *Configuring*, page *297*.

# Configuring

## General

### Number of Rules

The maximum number of rules that can be configured for an ACL is 1024.

### Order of Rules

The order of rules can affect packet handling! For e.g., if one rule dictates dropping of a packet while the *following* rule dictates mirroring to the CPU, and the packet meets the requirements of both rules, the *following* rule will be overriden by the previous rule, and the packet will be dropped without mirroring. If the order of these two rules is reversed, the packet will be mirrored rather than dropped.

### Compliance of Rules

Make sure when creating a rule it complies with the global profile (described in the section *Global Profiles*, page *295*).

## Creating a Rule

An ACL rule for packet handling is created in two stages:

Stage 1 – Packet Classification
Stage 2 – Actions on Packet

### Stage 1 – Packet Classification

Packet Classification is the specification of attribute values of packets (according to which the packets are to be forwarded or dropped). Examples of these attributes are: Protocol, Source IP address, Destination IP address, Source port, Destination port, etc.

#### *Ingress Ports and VLAN Interfaces*

To perform Stage 1 (packet classification) of any rule for *ingress* ports and VLAN interfaces:

1. Create or access an ACL as described in the section *Creating/Accessing*, page *296*.
2. Create a rule index (ID) by invoking the following command:

   **`rule [RULE_NUM]`**
   where,

**[RULE_NUM]**: (optional) Index of rule. If this argument is not entered, the rule is indexed automatically, i.e., it is assigned a number that is a multiple of 10. Further, this number is the smallest number larger than any of the other indices of the existing rules in the ACL.
Rules are ordered by their index. A rule with lower index has higher priority. This fact is significant, as noted in the section *Order of Rules*, page *297*.

On creation of the rule, the **rule** mode is entered as indicated by the prompt `OS900(config-rule)#`. The rule just created does *not* contain packet classification (or actions). To include packet classification in the rule, continue with the steps below.

3. [Optional] Select the protocol of the packets by invoking the command:
   **protocol eq <0-255>|icmp|igmp|ip|tcp|udp**
   where,
   **eq**: Equal to
   **<0-255>**: Range of IDs of protocols from which one can be selected. The protocols associated with these IDs can be obtained using the Internet link http://www.iana.org/assignments/protocol-numbers.
   **icmp**: Internet Control Message Protocol (ID = 1)
   **igmp**: Internet Gateway Message Protocol (ID = 2)
   **tcp**: Transmission Control Protocol (ID = 6)
   **udp**: User Datagram Protocol (ID = 17)
4. [Optional] Select the source IP address of the packets by invoking the command:
   **source-ip eq A.B.C.D/M|any**
   where,
   **eq**: Equal to
   **A.B.C.D./M**: *Source* prefix (IP address/mask) to be matched. The mask can be up to 31 bits long.
   **any**: Any prefix is a match
5. [Optional] Select the destination IP of the packets by invoking the command:
   **dest-ip eq A.B.C.D/M|any**
   where,
   **eq**: Equal to
   **A.B.C.D./M**: *Destination* prefix (IP address/mask) to be matched. The mask can be up to 31 bits long.
   **any**: Any prefix is a match
6. [Optional] Select the TCP/UDP source port of the packets by invoking the command:
   **source-port eq PORT_RANGE**
   where,
   **eq**: Equal to
   **PORT_RANGE**: Port range. The valid range is 0 to 65535. The acceptable formats are:
   numeric – for specifying one port, e.g., 327
   numeric/mask – for specifying several ports.
   The mask can have any value in the range 0-16,
   e.g., 31897/12.

**Note**

In the above command, the mask is used to select a range of ports. The mask specifies the number of Most Significant Bits (MSBs) that are to be the same (fixed) for all port numbers in the range. A port number (entered in decimal format) is internally translated by the OS900 as a 16-digit binary number.

<u>Example 1</u>:

This example shows what ports are included in the range when a port number and mask are entered. For example, the port/mask 240/14 is translated into the 16-bit binary number **00000000111100**00 with a mask on the 14 MSBs – shown in bold. This is equivalent to the range of ports **00000000111100**00, **00000000111100**01, **00000000111100**10, and **00000000111100**11.

Example 2:

This example shows how to determine the argument values to use in order to select a range of ports between two numbers. Suppose the numbers are 32 and 127.

The binary equivalent of 32 is **1**00000. To get all the values between 32 and 63, all MSBs down to and including the **1** in **00000000001**00000 must be masked. Accordingly, the mask must be 16 – 5 = 11. Therefore, to specify this range of ports, in *one* rule invoke the command **`source-port eq 32/11`**.

The binary equivalent of 127 is **1**111111. To get all the values between 64 and 127, all the MSBs down to and including the leftmost **1** in **0000000001**111111 must be masked. Accordingly, the mask must be 16 – 6 = 10. Therefore, to specify this range of ports, in the *other* rule invoke the command **`source-port eq 127/10`**.

The following is a CLI screen capture of the commands.

```
rule 10
  protocol eq tcp
  source-port eq 32/11
rule 20
  protocol eq tcp
  source-port eq 127/10
```

7. [Optional] Select the TCP/UDP destination port(s) of the packets by invoking the command:

   **`dest-port eq PORT_RANGE`**

   where,

   **`eq`**: Equal to

   **`PORT_RANGE`**: Port range. The valid range is 0 to 65535. The acceptable formats are:

   a numeric – for specifying one port, e.g., 25
   numeric/mask – for specifying several ports.
   The mask can have any value in the range 0-16, e.g., 31897/10.

   The Note above on masks for the command **`source-port eq PORT_RANGE`** applies for the command **`dest-port eq PORT_RANGE`** as well.

8. [Optional] Select the DSCP value of the packet by invoking the command:

   **`dscp eq DSCP_HEX_VALUE [MASK_HEX_VALUE]`**

   where,

   **`eq`**: Equal to

   **`DSCP_HEX_VALUE`**: DSCP value. Any hexadecimal number in the range `0x0` to `0x3F` can be entered.

   **`[MASK_HEX_VALUE]`**: Mask of DSCP value. Only the hexadecimal number `0x3F` can be entered. The mask is used to select several DSCP values. The mask in binary format is compared to the DSCP value in binary format. In the positions of the 0s of the mask, the DSCP bits are permitted to be 0 or 1. For e.g., a DSCP value 0x 9C ( = 10011100) and mask 3F ( = 00111111) together are equivalent to the $2^2$ DSCP values: **10**011100, **01**011100, **00**011100, **11**011100.

   By default, i.e., if the packet *ethertype* is not specified, DSCP values apply for IPv4 as well as for IPv6 addresses. For them to apply for only one of them, refer to Step *12*, below.

9. [Optional] Select the VPT value of the packet by invoking the command:

   **`vpt eq <0-7>`**

   where,

**eq**: Equal to

**<0-7>**: Range of VPT values. Any value between 0 and 7 can be entered.

10. [Optional] Select the VLAN tag of the packet by invoking either of the following commands:

```
tag eq <1-4095> [MASK_HEX_VALUE]
tag eq <0-4095> up-to <1-4095>
ctag eq <0-4095> up-to <1-4095>
```

where,

**tag**: For single-tag packets

**ctag**: For double-tag packets

**eq**: Equal to

**up-to**: range

**<1-4095>**: (First appearance) (Lowest) VLAN tag of packet (in the range).

**<1-4095>**: (Second appearance) Highest VLAN tag of packet in the range.

**[MASK_HEX_VALUE]**: Mask hex value in the hexadecimal range **0** to **fff**. Allows for selecting a range of VLAN tags. A '0' binary digit in the mask means that the VLAN tag binary digit in the same position will be considered as '0' and '1' to give two values. For example, if the VLAN tag is decimal 9, i.e., binary 1001, and the mask is hex C, i.e., binary 1100, the *range* of VLAN tags is 10**00** *to* 10**11**, i.e., decimal 8 to 11.

The advantage in using the rule classification command with the keyword **up-to** is that it takes up only one rule space instead of several. If the lowest VLAN tag of the range is not a number that can be expressed as an integral power of 2, the OS900 automatically rounds up the entered tag to the greatest number smaller than the entered tag that can be expressed as an integral power of 2. If the highest VLAN tag of the range is not a number that can be expressed as an integral power of 2, the OS900 automatically rounds up the entered tag to the smallest number greater than the entered tag that can be expressed as an integral power of 2. For example, if the entered lowest VLAN tag value is 21, it is rounded down to 16. If the entered highest VLAN tag value is 58, it is rounded up to 63.

11. [Optional] Select the VLAN tag of the packet by invoking the command:

```
tag eq <1-4095>|any|untagged [MASK_HEX_VALUE]
```

where,

**eq**: Equal to

**<1-4095>**: VLAN tag of packet.

**any**: All tagged packets

**untagged**: All untagged packets

**[MASK_HEX_VALUE]**: Mask hex value in the hexadecimal range **0** to **fff**. Allows for selecting a range of VLAN tags. A '0' binary digit in the mask means that the VLAN tag binary digit in the same position will be considered as '0' and '1' to give two values. For example, if the VLAN tag is decimal 9, i.e., binary 1001, and the mask is hex C, i.e., binary 1100, the *range* of VLAN tags is 10**00** *to* 10**11**, i.e., decimal 8 to 11.

12. [Optional] Specify the packet *ethertype* (follows the VLAN header) by invoking the command:

```
ethertype eq ETHERTYPE
```

where,

**eq**: Equal to

**ETHERTYPE**: Ethertype value in the range [0x5dd to 0xffff] and different from the port core-ethertype

For DSCP to relate to IPv4 addresses only, set the ethertype value to **0x800**.

For DSCP to relate to IPv6 addresses only, set the ethertype value to **0x86dd**.

13. [Optional] Specify the *source* MAC address for non IP/ARP packets by invoking the command:

**src-mac-addr-for-non-ip eq MAC_ADDRESS [MASK]**

where,

**eq**: Equal to

**MAC_ADDRESS**: *Source* MAC address in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

**[MASK]**: Mask in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

14. [Optional] Specify the *destination* MAC address for non IP/ARP packets by invoking the command:

**dest-mac-addr-for-non-ip eq MAC_ADDRESS [MASK]**

where,

**eq**: Equal to

**MAC_ADDRESS**: *Destination* MAC address in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

**[MASK]**: Mask in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

15. [Optional] Specify the source physical port (irrespective of whether the port is a member of a VLAN interface) by invoking the command:

**src-phy-port eq PORT**

where,

**eq**: Equal to

**PORT**: Physical port number

16. [Optional] Specify the packet TCP flags by invoking the command:

**tcp-flags eq HEX_VALUE [MASK_HEX_VALUE]**

where,

**eq**: Equal to

**HEX_VALUE**: TCP flags [0x0 to 0x3f] (URG = 0x20, ACK = 0x10,PSH = 0x8, RST = 0x4, SYN = 0x2, FIN = 0x1)

**[MASK_HEX_VALUE]**: Mask value for TCP flags [0x0 to 0x3f]

17. [Optional] Specify the value of the EXP bits of MPLS packets (on whom one or more actions are to be performed) by invoking the command:

For Tagged Packets

**mpls-exp-tagged eq <0-7>**

where,

**eq**: Equal to

**<0-7>**: EXP value

To revoke a *specific* value of the EXP bits of *tagged* MPLS packets (and therefore the action/s to be performed on such packets), invoke the command:

**no mpls-exp-tagged eq <0-7>**

where,

**eq**: Equal to

**<0-7>**: EXP value

To revoke *all* values of the EXP bits of MPLS *tagged* packets (and therefore the action/s to be performed on such packets), invoke the command:

**no mpls-exp-tagged**

For Untagged Packets

**mpls-exp-untagged eq <0-7>**

where,

**eq**: Equal to

**<0-7>**: EXP value

To revoke a *specific* value of the EXP bits of *untagged* MPLS packets (and therefore the action/s to be performed on such packets), invoke the command:

**no mpls-exp-untagged eq <0-7>**

where,

**eq**: Equal to

**<0-7>**: EXP value

To revoke *all* values of the EXP bits of MPLS *untagged* packets (and therefore the action/s to be performed on such packets), invoke the command:

**no mpls-exp-untagged**

| | Note |
|---|---|
| | Classification according to EXP bits (using the command **mpls-exp-tagged eq <0-7>** or **mpls-exp-untagged eq <0-7>**) cannot be combined with classification according to L3 or L4 in the same rule!<br>An ACL with classification according to EXP bits cannot be bound to *egress* ports. |

18. If required, create additional rules by repeating steps *2* to *15* above for each rule.

***Egress Ports***

To perform Stage 1 (packet classification) of any rule for *egress* ports:

1. Create or access an ACL as described in the section *Creating/Accessing*, page *296*.
2. Create a rule index (ID) by invoking the following command:

   **rule [RULE_NUM]**

   where,

   **[RULE_NUM]**: (optional) Index of rule. If this argument is not entered, the rule is indexed automatically, i.e., it is assigned a number that is a multiple of 10. Further, this number is the smallest number larger than any of the other indices of the existing rules in the ACL.
   Rules are ordered by their index. A rule with lower index has higher priority. This fact is significant, as noted in the section *Order of Rules*, page *297*.

   On creation of the rule, the **rule** mode is entered as indicated by the prompt `OS900(config-rule)#`. The rule just created does *not* contain packet classification (or actions). To include packet classification in the rule, continue with the steps below.
3. [Optional] Select the protocol of the packets by invoking the command:

   **protocol eq <0-255>|icmp|igmp|ip|tcp|udp**

   where,

   **eq**: Equal to

   **<0-255>**: Range of IDs of protocols from which one can be selected. The protocols associated with these IDs can be obtained using the Internet link http://www.iana.org/assignments/protocol-numbers.

   **icmp**: Internet Control Message Protocol (ID = 1)

   **igmp**: Internet Gateway Message Protocol (ID = 2)

   **tcp**: Transmission Control Protocol (ID = 6)

   **udp**: User Datagram Protocol (ID = 17)
4. [Optional] Select the source IP address of the packets by invoking the command:

   **source-ip eq A.B.C.D/M|any**

   where,

   **eq**: Equal to

   **A.B.C.D./M**: *Source* prefix (IP address/mask) to be matched. The mask can be up to 31 bits long.

   **any**: Any prefix is a match
5. [Optional] Select the destination IP of the packets by invoking the command:

   **dest-ip eq A.B.C.D/M|any**

   where,

   **eq**: Equal to

   **A.B.C.D./M**: *Destination* prefix (IP address/mask) to be matched. The mask can be up to 31 bits long.

**any**: Any prefix is a match

6. [Optional] Select the DSCP value of the packet by invoking the command:

   **dscp eq DSCP_HEX_VALUE [MASK_HEX_VALUE]**

   where,

   **eq**: Equal to

   **DSCP_HEX_VALUE**: DSCP value. Any hexadecimal number in the range `0x0` to `0x3F` can be entered.

   **[MASK_HEX_VALUE]**: Mask of DSCP value. Any hexadecimal number in the range `0x0` to `0xFF` can be entered. The mask is used to select several DSCP values. The mask in binary format is compared to the DSCP value in binary format. In the positions of the 0s of the mask, the DSCP bits are permitted to be 0 or 1. For e.g., a DSCP value 0x 9C ( = 10011100) and mask FD ( = 11101101) together are equivalent to the $2^2$ DSCP values: 100**1**11**0**0, 100**0**11**1**0, 100**1**11**1**0, 100**0**11**0**0.

7. [Optional] Select the VPT value of the packet by invoking the command:

   **vpt eq <0-7>**

   where,

   **eq**: Equal to

   **<0-7>**: Range of VPT values. Any value between 0 and 7 can be entered.

8. [Optional] Select the VLAN tag of the packet by invoking the command:

   **tag eq <1-4095>|any|untagged [MASK_HEX_VALUE]**

   where,

   **eq**: Equal to

   **<1-4095>**: VLAN tag of packet.

   **any**: All tagged packets

   **untagged**: All untagged packets

   **[MASK_HEX_VALUE]**: Mask hex value in the hexadecimal range **0** to **fff**. Allows for selecting a range of VLAN tags. A '0' binary digit in the mask means that the VLAN tag binary digit in the same position will be considered as '0' and '1' to give two values. For example, if the VLAN tag is decimal 9, i.e., binary 1001, and the mask is hex C, i.e., binary 1100, the *range* of VLAN tags is 10**00** *to* 10**11**, i.e., decimal 8 to 11.

9. [Optional] Specify the packet *ethertype* (follows the VLAN header) by invoking the command:

   **ethertype eq ETHERTYPE**

   where,

   **eq**: Equal to

   **ETHERTYPE**: Ethertype value in the range [`0x5dd` to `0xffff`] and different from the port core-ethertype

   **Note**

   Packets assigned *ethertype* **0x806** (ARP) can neither be distinguished by the classification **source-ip** (source IP address) nor by the classification **dest-ip** (destination IP address).

10. [Optional] Specify the *source* MAC address for non IP/ARP packets by invoking the command:

    **src-mac-addr-for-non-ip eq MAC_ADDRESS [MASK]**

    where,

    **eq**: Equal to

    **MAC_ADDRESS**: *Source* MAC address in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

    **[MASK]**: Mask in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

11. [Optional] Specify the *destination* MAC address for non IP/ARP packets by invoking the command:

    **dest-mac-addr-for-non-ip eq MAC_ADDRESS [MASK]**

where,

**eq**: Equal to

**MAC_ADDRESS**: *Destination* MAC address in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

**[MASK]**: Mask in hex format (e.g., `aa:bb:cc:dd:ee:ff`)

12. If required, create additional rules by repeating steps *2* to *15* above for each rule.

### Stage 2 – Actions on Packet

Actions for a rule consist of selecting one or more actions (to be performed on a packet) conditional on the packet classification (Stage 1) and the command **action deny|permit** (described in the subsections, *Ingress Ports and VLAN Interfaces* and *Egress Ports*, below).

Stage 2 may be performed immediately after completing Stage 1, above, while in **rule** mode. **rule** mode is indicated by the prompt `OS900(config-rule)#`, and is applicable for the rule that is the instance (current).

The SL value assigned in Stage 2 (using any of actions *3.5* to *3.13* and *3.19*, in the section *Ingress Ports and VLAN Interfaces*, below) overrides the SL assigned as described in the section *Custom Map*, page *363*.

In Stage 2, an action (or Action List) that is the instance (current) can be deleted, by invoking the command:

**no action**

<u>Example</u>

```
OS900(config-rule)# action mark sl 7 vpt 3
OS900(config-rule)# show
OS910(config-rule)# show
Rule index: 10
 Action:
  Mark sl 7
  Mark vpt 3
 Rule:
  Rule is enable.
----------
OS910(config-rule)# no action mark sl
OS910(config-rule)# show
Rule index: 10
 Action:
  Mark vpt 3
 Rule:
  Rule is enable.
----------
OS910(config-rule)#
```

In the above example, the command '**no action mark sl**' revokes only the action '`Mark sl 7`'. To revoke all actions of a rule, invoke the command: **no action all**.

Up to 56 *mark* actions can be defined per ACL. A mark action can include one or more of the following packet attributes: VPT, DSCP, and SL.

#### *Ingress Ports and VLAN Interfaces*

To perform Stage 2 (action on packets) of any rule for *ingress* ports and VLAN interfaces:

1. Enter **rule** mode of the specific rule. This may require performance of the following sequence of actions: entry into **enable** mode, entry into **configure terminal** mode, entry into **access-list** mode for the specific ACL (as described in the section *Creating/Accessing*, page *296*.), entry into **rule** mode of the specific rule (as described in step *2*, page *297*).
2. Invoke the command[39]:

[39] This command (action) may be overridden if a rule with a lower index number specifies a conflicting action – see the section *Order of Rules*, page *297*.

**`action deny|permit`**

where,

**`deny`**: Deny (*drop*) packets that have all the attribute values (specified in *Stage 1 – Packet Classification*, page *297*) .

**`permit`**: Permit (*forward*) packets that have all the attribute values.

> **Note**
> The actions in steps *3.1* to *3.10* are conditional on the command **`action deny|permit`**.

3. Select any *one* or more of the following actions, provided they do not conflict with one another:

3.1. *Trap/copy* packets to the CPU by invoking the command:

**`action (trap-to-cpu [high-priority]|mirror-to-cpu)`**

where,

**`trap-to-cpu`**: *Trap* (send) packets only to the CPU.

**`high-priority`**: With high priority.

**`mirror-to-cpu`**: *Copy* packets to the CPU.

3.2. If a rate limit is required for traffic to the CPU, *trap/copy* the packets to the CPU by invoking the command:

**`action redirect port cpu`**

3.3. *Copy* packets to the analyzer port/VLAN by invoking the command:

**`action mirror-to-analyzer`**

where,

**`mirror-to-analyzer`**: *Copy* packets to the analyzer port/VLAN.

3.4. *Loopback and swap* MAC SA with MAC DA by invoking the command:

**`action layer2-loopback port PORT`**

where,

**`PORT`**: The number of the port to which the packet is to be sent.

3.5. Mark packets with an SL value by invoking the command:

**`action mark sl <1-8>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

> **Note**
> The effect of SL marking depends on the binding of the ACL (using the command **`access-group`**). When an ACL is bound to an interface or port, the marking sets the internal SL used for ingress shaping. In order for the marking action to effect the actual egress SL, the ACL should be bound to a port using the command **`port access-group extra`** …).

3.6. Mark packets with a DSCP value by invoking the command:

**`action mark dscp <0-63>`**

where,

**`mark`**: Marking.

**`dscp`**: DSCP.

**`<0-63>`**: Range of DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

3.7. Mark packets with a VPT value by invoking the command:

**action mark vpt <0-7>**

where,

**mark**: Marking.

**vpt**: VPT.

**<0-7>**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

> **Note**
>
> The effect of VPT marking depends on the binding of the ACL (using the command **access-group**) and the ingress port tag-outbound mode. When ACL is bound to an interface or to a port, the VPT marking is effective only if the ingress port is *not* set as 'untagged'. In order for the marking action to effect the actual egress packet when ingress port is'untagged,' the ACL should be bound to a port using the command **port access-group extra** …).

3.8. Redirect all packets that enter ports (even trunk ports) in a VLAN to a specific port in the VLAN by invoking the command:

**action redirect port PORT**

where,

**PORT**: Port number.

3.9. Swap (replace) the VLAN tag of ingress packets by invoking the command:

**action tag swap <0-4095>**

where,

**<0-4095>**: Range of VLAN tags from which one tag is to be selected.

> **Note**
>
> In combination with the command **port tag-outbound-mode q-in-q PORTS-GROUP TAG** (described in the section *Q-in-Q (Service* VLAN *Access* Mode), page *138*), this action can be used to implement selection of a specific service VLAN in Provider Bridges applications.

3.10. Translate/swap the *customer* VLAN tag of packets (for the *service* VLAN tag) by invoking the command:

**action tag swap-ctag <0-4095> stag <0-4095>**

where,

**<0-4095>**: (First appearance) Range of *customer* VLAN tags from which one tag is to be selected.

**<0-4095>**: (Second appearance) Range of *service* VLAN tags from which one tag is to be selected.

3.11. Assign a specific Action List by invoking the command:

**action list NAME**

where,

**NAME**: *Action* List name.

3.12. Nest a tag (add a higher level tag, e.g., an IEEE802.1ad q-in-q service provider bridge tag) to an incoming packet by invoking the command:

**action tag nest <0-4095> [vpt <0-7>]**

where,

**<0-4095>**: Range of VLAN tags from which one tag is to be selected.

**[vpt]**: (Optional) VLAN priority tag.

**<0-7>**: Range of VLAN priority tags from which one tag is to be selected.

3.13. Swap the VLAN tag and VPT value of packets by invoking the command:

**`action tag swap <0-4095> vpt <0-7>`**

where,

**`<0-4095>`**: Range of VLAN tags from which one tag is to be selected.

**`<0-7>`**: Range of VLAN priority values from which one value is to be selected.

3.14. Mark packets with an SL and DSCP value by invoking the command:

**`action mark sl <1-8> dscp <0-63>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. If an SL value already exists, it is overwritten.

**`dscp`**: DSCP.

**`<0-63>`**: Range of DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

3.15. Mark packets with an SL and VPT value by invoking the command:

**`action mark sl <1-8> vpt <0-7>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

**`vpt`**: VPT.

**`<0-7>`**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

3.16. Mark packets with an SL, DSCP, and VPT value by invoking the command:

**`action mark sl <1-8> dscp <0-63> vpt <0-7>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

**`dscp`**: is a keyword signifying DSCP.

**`<0-63>`**: DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

**`vpt`**: keyword signifying VPT.

**`<0-7>`**: Range of VPT values from which one can be selected. If a VPT value already exists, it is overwritten.

3.17. Mark packets with an SL value and *swap their VLAN tag* by invoking the command:

**`action mark sl <1-8> tag swap <0-4095>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

**`tag swap`**: Swap VLAN tag

**`<0-4095>`**: Range of VLAN tags from which one tag is to be selected.

3.18. Mark packets with an SL and VPT value and *swap their VLAN tag* by invoking the command:

**`action mark sl <1-8> vpt <0-7> tag swap <0-4095>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

**`vpt`**: VPT.

**`<0-7>`**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

**`tag swap`**: Swap VLAN tag

**`<0-4095>`**: Range of VLAN tags from which one tag is to be selected.

3.19. Mark packets with an *SL* and *DSCP* value and *swap* the VLAN tag of the packets by invoking the command:

**`action mark sl <1-8> dscp <0-63> tag swap <0-4095>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. If an SL value already exists, it is overwritten.

**`dscp`**: DSCP.

**`<0-63>`**: Range of DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

**`tag swap`**: Swap VLAN tag

**`<0-4095>`**: Range of VLAN tags from which one tag is to be selected.

3.20. Mark packets with an SL, DSCP, VPT value, and *swap their VLAN tag* by invoking the command:

**`action mark sl <1-8> dscp <0-63> vpt <0-7> tag swap <0-4095>`**

where,

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

**`dscp`**: DSCP.

**`<0-63>`**: Range of DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

**`vpt`**: VPT.

**`<0-7>`**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

**`tag swap`**: Swap VLAN tag

**`<0-4095>`**: Range of VLAN tags from which one tag is to be selected.

3.21. Assign a specific Action List and, optionally, mark ingress packets with an SL, DSCP, VPT value, and *swap their VLAN tag* by invoking the command:

**`action list NAME [mark [sl <1-8>] [dscp <0-63>] [vpt <0-7>] [tag swap <0-4095>]]`**

where,

**`NAME`**: *Action* List name.

**`mark`**: Marking.

**`sl`**: SL.

**`<1-8>`**: Range of SL values from which one can be selected. (If an SL value already exists, it is overwritten.)

**`dscp`**: DSCP.

**`<0-63>`**: Range of DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

**`vpt`**: VPT.

**`<0-7>`**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

**`tag swap`**: Swap VLAN tag

**`<0-4095>`**: Range of VLAN tags from which one tag is to be selected.

3.22. It is possible that no rule will apply to certain packet types. Such packets, by default, are dropped. To enable forwarding (or dropping) of all such packets:

3.22.1. Enter the **`access-list`** mode of the ACL.
To do so when in the **`rule`** mode, invoke the command **`exit`**.
(To do so when in the **`configure terminal`** mode, invoke the command **`access-list extended WORD`**, where **`WORD`** is the name of the ACL.)

3.22.2. Invoke the command:

**`default policy permit|deny`**

where,

**`permit`**: *Permit* forwarding of a packet if no rule applies.

**`deny`**: Drop (*deny* forwarding of) a packet if no rule applies.

Example

```
OS900(config-access-list)# default policy permit
OS900(config-access-list)#
```

***Egress Ports***

To perform Stage 2 (action on packets) of any rule for *egress* ports:

1. Enter **`rule`** mode of the specific rule. This may require performance of the following sequence of actions: entry into **`enable`** mode, entry into **`configure terminal`** mode, entry into **`access-list`** mode for the specific ACL (as described in the section *Creating/Accessing*, page *296*.), entry into **`rule`** mode of the specific rule (as described in step *2*, page *297*).
2. Invoke the command[40]:

**`action deny|permit`**

where,

**`deny`**: Deny (*drop*) packets that have all the attribute values (specified in *Stage 1 – Packet Classification*, page *297*) .

**`permit`**: Permit (*forward*) packets that have all the attribute values.

| | |
|---|---|
| | **Note**<br>The actions in steps *3.1* to *3.10* are conditional on the command **`action deny|permit`**. |

3. Select any *one* or more of the following actions, provided they are not mutually conflictual:

[40] This command (action) may be overridden if a rule with a lower index number specifies a conflicting action – see the section *Order of Rules*, page *297*.

> **Note**
> Before invoking the command **action mark** … **vpt** or **action tag swap** … for a port, first make sure that the port is set in **tagged** or **hybrid** mode and the rule action **permit** has been selected.

3.1. Mark packets with a DSCP value by invoking the command:

**action mark dscp <0-63>**

where,

**mark**: Marking.

**dscp**: DSCP.

**<0-63>**: Range of DSCP values from which one can be selected. (If a DSCP value already exists, it is overwritten.)

> **Note**
> The **action mark** … **dscp** can apply only to IP packets. For it to apply to non-IP packets as well, the non-IP packets must be assigned the *ethertype* **0x800** (for IPv4 packets) or **0x86dd** (for IPv6 packets) using the command **ethertype eq ETHERTYPE**.

3.2. Mark packets with a VPT value by invoking the command:

**action mark vpt <0-7>**

where,

**mark**: Marking.

**vpt**: VPT.

**<0-7>**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

> **Note**
> The effect of VPT marking depends on the binding of the ACL (using the command **access-group**) and the ingress port tag-outbound mode. When ACL is bound to an interface or to a port, the VPT marking is effective only if the ingress port is *not* set as 'untagged'. In order for the marking action to effect the actual egress packet when ingress port is'untagged,' the ACL should be bound to a port using the command **port access-group extra** …).

3.3. Swap (replace) the VLAN tag of packets by invoking the command:

**action tag swap <0-4095>**

where,

**<0-4095>**: Range of VLAN tags from which one tag is to be selected.

> **Note**
> In combination with the command **port tag-outbound-mode q-in-q PORTS-GROUP TAG** (described in the section *Q-in-Q (Service* VLAN *Access* Mode), page *138*), this action can be used to implement selection of a specific service VLAN in Provider Bridges applications.

3.4. Swap the VLAN tag and VPT value of egress packets by invoking the command:

**action tag swap <0-4095> vpt <0-7>**

where,

**<0-4095>**: Range of VLAN tags from which one tag is to be selected.

**<0-7>**: Range of VLAN priority values from which one value is to be selected.

3.5. It is possible that no rule will apply to certain packet types. Such packets, by default, are dropped. To enable forwarding (or dropping) of all such packets:

3.5.1. Enter the **access-list** mode of the ACL.
To do so when in the **rule** mode, invoke the command **exit**.
(To do so when in the **configure terminal** mode, invoke the command **access-list extended WORD**, where **WORD** is the name of the ACL.)

3.5.2. Invoke the command:

**default policy permit|deny**

where,

**permit**: *Permit* forwarding of a packet if no rule applies.

**deny**: Drop (*deny* forwarding of) a packet if no rule applies.

Example

```
OS900(config-access-list)# default policy permit
OS900(config-access-list)#
```

## Viewing a Rule

To view a *specific* rule of an ACL:

1. Enter **configure terminal** mode.
2. Enter the mode of the ACL whose rule(s) is/are to be viewed by invoking the command:

   **access-list extended WORD**

   where,

   **WORD**: Name of the ACL
3. Invoke the command:

   **show rule RULE_NUM**

   where,

   **[RULE_NUM]** : Index of rule.

Example

```
OS900# configure terminal
OS900(config)# access-list extended ACL1
OS900(config-access-list)# show rule 10
Rule index: 10
Action:deny
Source ip:32.32.32.32/32
----------
OS900(config-access-list)#
```

To view *all* rules of an ACL:

1. Enter **configure terminal** mode.
2. Enter the mode of the ACL whose rule(s) is to be viewed by invoking the command:

   **access-list extended WORD**

   where,

   **WORD**: Name of the ACL
3. Invoke the command:

   **show**

Example

```
OS900# configure terminal
OS900(config)# access-list extended ACL1
OS900(config-access-list)# show

Access List Extended ACL1
=========================
```

```
state: NOT ACTIVE
----------
Rule index: 10
Action:deny
Source ip:32.32.32.32/32
----------
Rule index: 20
Action:permit
Destination ip:31.31.31.0/24
----------
Rule index: 30
Action:action-list ACN1 with mark sl 7
----------
Rule index: 40
Action:action-list ACN1
Protocol:icmp
----------
default policy: deny all
OS900(config-access-list)#
```

## Editing a Rule

To edit an existing or new rule:

1. Invoke the command:

   **`rule RULE_NUM`**

   where,

   **`RULE_NUM`**: Index of the rule to be edited

   Example

   ```
   OS900(config)# access-list extended Sales
   OS900(config-access-list)#
   OS900(config-access-list)# rule 2
   OS900(config-rule)#
   ```

2. Invoke any one or more of the commands noted above for classification and actions.

## Moving a Rule

To move a rule, invoke the command:

**`rule RULE_NUM move NEW_RULE_NUM`**

where,

**`RULE_NUM`**: Index of the rule to be moved

**`NEW_RULE_NUM`**: New index to be assigned to the rule. The rule is moved to a position so that the indexes of all the rules are in ascending order from top to bottom.

Example

```
OS900(config-access-list)#
OS900(config-access-list)# rule 3 move 1
OS900(config-access-list)#
```

## Enabling a Rule

By default, a rule is enabled. To enable a *specific* rule:

1. Enter the **`access-list`** mode of the ACL.
2. Enter the mode of the rule to be enabled.
3. Invoke the command:

   **`enable`**

Example

```
OS912C(config)# access-list extended ACL1
OS912C(config-access-list)# rule 30
OS912C(config-rule)# enable

OS912C(config-rule)# show
Rule index: 30
 Action:
 Rule:
  Rule is enable.
----------
OS912C(config-rule)#
```

## Disabling a Rule

To disable a *specific* rule:

1. Enter the **access-list** mode of the ACL.
2. Enter the mode of the rule to be disabled.
3. Invoke the command:
   **no enable**

Example

```
OS912C(config)# access-list extended ACL1
OS912C(config-access-list)# rule 30
OS912C(config-rule)# no enable

OS912C(config-rule)# show
Rule index: 30
 Action:
 Rule:
  Rule is disable.
----------
OS912C(config-rule)#
```

## Deleting a Rule

To delete a *specific* rule:

1. Enter the **access-list** mode of the ACL.
2. Invoke the command:
   **no rule RULE_NUM**
   where,
   **RULE_NUM**: Index of the rule.

Example

```
OS900(config-access-list)#
OS900(config-access-list)# no rule 2
OS900(config-access-list)#
```

To delete *all* rules of an ACL:

1. Enter the **access-list** mode of the ACL.
2. Invoke the command:
   **flush**

Example

```
OS900(config)# access-list extended ACL1
OS900(config-access-list)# flush
OS900(config-access-list)#
```

# ARP Packets

To enable the destination (or source) IP address of ARP packets to be compared with that defined in a rule for the purpose of forwarding/dropping, an additional rule must be created. This rule must include:

1. The same IP address of the ARP packets as that in the rule specifying the IP address of ARP packets
2. The action 'permit'
3. ARP packets' *ethertype* (**`0x806`**)

Example:

```
!
access-list extended ACL1
rule 20
  dest-ip eq 9.8.6.0/24
  action permit

 rule 10
  action permit
  dest-ip eq 9.8.6.0/24
  ethertype eq 0x806
```

In the above example, the additional rule is '`rule 10`'. Note that this rule is given a lower index (higher priority) to emphasize that it is not to be overridden by some other rule in the ACL.

# Global Default Policy

A packet-handling policy (called Global Default Policy) that applies to *all* ACLs configured on the OS900 can be implemented. This policy can be either 'permit forwarding' or 'deny forwarding' (of a packet if it does not *possess* any of the attributes specified in the rules of the associated ACL.

To implement a Global Default Policy:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`access-list extended-default-policy deny|permit`**

   where,

   **`deny`**: Drop a packet if any criterion for forwarding the packet in any rule is not met.

   **`permit`**: Forward a packet if no criterion for forwarding the packet in any rule is violated.

**Note**

The command Global Default Policy is effective for ACLs that are bound *after* invocation of this command. To make the command Global Default Policy effective for an ACL that is bound *before* invocation of this command, unbind *all* ACLs, invoke the command Global Default Policy, and then rebind the ACL.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# access-list extended-default-policy permit
OS900(config)#
```

# Viewing

Configured ACLs can be viewed from any of the following modes:

- **access-list** mode
- **enable** mode

__**access-list** mode__

Only the current ACL can be displayed from this mode. To display the ACL, invoke the command:

**show [detail]**

where,

**detail** (optional): Information in detail. The command without this argument displays abbreviations used by the OS900 in displaying rule actions.

__Example__

```
OS900(config-access-list)# show

Access List Extended ACL2
=========================
state: NOT ACTIVE
----------
default policy: deny all
OS900(config-access-list)#
```

__**enable** mode__

Any one or more ACLs can be displayed from this mode.

**show access-list [NAME|configuration]**

where,

**NAME**: (Optional) Name of an existing ACL. The command displays a specific ACL if the ACL name is typed in place of this argument. The command without this argument displays all the ACLs in memory.

**configuration**: ACLs in run-time memory.

__Example__

```
OS900# show access-list ACL2

Access List Extended ACL2
=========================
state: NOT ACTIVE
----------
default policy: deny all
OS900#
```

# Comment Adding

A user comment on an ACL can be entered with the ACL as follows:

1. Enter the **access-list** mode of the ACL.
2. Invoke the command:

   **remark LINE**

   where,

   **LINE**: Comment on the current ACL.

__Example__

```
OS900> enable
OS900# configure terminal
OS900(config)# access-list extended ACL1
OS900(config-access-list)# remark This ACL is to be used for the Sales Dept.
OS900(config-access-list)# show

Access List Extended ACL2
```

```
========================
This ACL is to be used for the Sales Dept.
state: NOT ACTIVE
----------
default policy: deny all
OS900(config-access-list)#
```

# Binding

## Limitations

– Only one ACL can be bound to a VLAN interface.

– Up to two ACLs can be bound to a regular port[41] one for *ingress* traffic and one for *egress* traffic.

– Up to three ACLs can be bound to a dual port[42]; one to the *internal* port and two to the *external* port; one for ingress traffic and one for egress traffic.

– A specific ACL can be bound either to *ingress ports/VLANs* or *egress ports*; not both.

## Ingress Ports and Ingress VLAN Interfaces

### Mode

Ingress ports can be configured to use ACLs in either of the following modes:

– Port Mode

– VLAN Mode

In Port Mode, incoming packets are handled according to the ACL bound to the port group. In VLAN Mode, incoming packets are handled according to the ACL bound to the VLAN interface having the same tag as the packet. (In VLAN Mode, an ingress port must be a member of the VLAN interface otherwise the packets may be dropped depending on the handling mode set as described in the section *Outbound Tag Mode*, page *137*.)

To select the binding mode and to bind ACLs to a port group:

1. Enter **configure terminal** mode.
2. Select Port Mode or VLAN Mode by invoking the command:

   **port acl-binding-mode by-port|by-vlan [PORTS-GROUP]**

   where,

   **by-port**: (Port Mode) Use ACL bound to a port group.

   **by-vlan**: (VLAN Mode) Use ACL bound to VLAN interface having the same tag as the incoming packet. (Default).

   **PORTS-GROUP**: Group of ports.

### Ingress Ports

1. To bind an ACL to an ingress port group, invoke the command:

   **port access-group WORD PORTS-GROUP**

   where,

   **WORD**: Name of ACL.

   **PORTS-GROUP**: Group of Ports.

2. Two ACLs may be bound to a port group. The first ACL is bound as in step *1*, above. To bind a *second* ACL to a port group, invoke the command:

---

[41] A regular port consists of one external port.

[42] A dual port consists of one external port and one internal port. For details, refer to section *Regular, Dual, and Extra Internal* Ports, page *155*.

**`port access-group extra WORD PORTS-GROUP`**

where,

**`WORD`**: Name of *second* ACL.

**`PORTS-GROUP`**: *Same* group of Ports as for the first ACL. (The port/s must not be port 11 or 12 of the OS912.)

**Ingress VLAN Interface**

To bind an ACL to a VLAN interface:

1. Invoke the command:

   **`interface vlan IFNAME`**

   where,

   **`IFNAME`**: ID of the interface, e.g., **`vif1`**, **`vif2`**, etc.

2. From the VLAN interface's mode, invoke the command:

   **`access-group WORD`**

   where,

   **`WORD`**: Name of the ACL.

**Example**

--------------------------------------Configuring Interface vif777--------------------------------------

```
OS900(config)# interface vlan vif777
OS900(config-vif777)# ports 1,2
OS900(config-vif777)# tag 7
Interface is activated.

OS900(config)# show port access-list
  [PORT-GROUP]  Group of Ports
  |             Output modifiers
OS900(config)# show port access-list

  Port Access List Configuration
 ================================
 Port   Binding Mode   Access List   Extra ACL     Egress ACL
--------------------------------------------------------------
    1     by-vlan
    2     by-port
    3     by-vlan
    4     by-vlan
OS900(config)#
```

-------------------------Selecting the mode for binding an ACL to Port 2-------------------------

```
OS900(config-vif777)# exit
OS900(config)# port acl-binding-mode ?
  by-port  Set acl binding by port
  by-vlan  Set acl binding by vlan
OS900(config)# port acl-binding-mode by-port ?
  <cr>
  PORTS-GROUP  Group of Ports
  |            Output modifiers
OS900(config)# port acl-binding-mode by-port 2 ?
  <cr>
  |     Output modifiers
OS900(config)# port acl-binding-mode by-port 2
```

----------------------------Displaying the binding modes for each port-----------------------------

```
OS900(config)# show port access-list
```

```
  Port Access List Configuration
 ================================
 Port   Binding Mode   Access List   Extra ACL     Egress ACL
--------------------------------------------------------------
    1     by-vlan
    2     by-port
    3     by-vlan
    4     by-vlan
OS900(config)#

     -------------------------------------Binding ACL ACL6 to Port 2--------------------------------------

OS900(config)# port access-group ACL6 2
OS900(config)#

     ---------------------------------Binding ACL ACL7 also to Port 2------------------------------------

OS900(config)# port access-group extra ACL7 2
OS900(config)#

     ------------------------------Binding ACL ACL8 to Interface vif777--------------------------------

OS900(config)# interface vif777
OS900(config-vif777)# access-group ACL8
OS900(config-vif777)#
```

### Egress Ports

ACLs can be bound to *egress* ports only; not *egress* VLANs
To bind an ACL to an egress port group:

1. Enter **configure terminal** mode.
2. Select Port Mode by invoking the command:
   **port acl-binding-mode by-port [PORTS-GROUP]**
   where,
   **by-port**: (Port Mode) Use ACL bound to a port group.
   **PORTS-GROUP**: Group of ports.
3. Invoke the command:
   **port access-group egress WORD PORTS-GROUP**
   where,
   **WORD**: Name of ACL.
   **PORTS-GROUP**: Group of ports.

## Unbinding

### Ingress Ports

To unbind the *first* ACL from a *group of ports*:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no port access-group PORTS-GROUP**
   where,
   **PORTS-GROUP**: Group of Ports.

Example

```
OS900# configure terminal
OS900(config)# no port access-group 4
OS900(config)#
```

To unbind the *second* ACL from a *group of ports*:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no port access-group extra PORTS-GROUP**
   where,
   **PORTS-GROUP**: *Same* group of Ports.

Example

```
OS900# configure terminal
OS900(config)# no port access-group extra 4
OS900(config)#
```

## Ingress VLAN Interface

To unbind an ACL from an *ingress VLAN interface*:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **interface IFNAME**
   where,
   **IFNAME**: ID of the interface, e.g., **vif1**, **vif2**, etc.
3. Invoke the command:
   **no access-group**

Example

```
OS900# configure terminal
OS900(config)# interface vif777
OS900(config-vif777)# no access-group
OS900(config-vif777)#
```

## Egress Ports

To unbind an ACL from an *egress* port group:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no port access-group egress PORTS-GROUP**
   where,
   **PORTS-GROUP**: Group of ports.

Example

```
OS900(config)# port access-group ACL3 1,3
OS900(config)#
```

# Deleting

To delete an ACL:

1. Unbind the ACL from *each* interface to which it has been bound as described in the section *Unbinding*, page *318*.
2. Enter **configure terminal** mode.
3. Invoke the command:
   **no access-list WORD**
   where,
   **WORD**: Name of the ACL

Example

```
OS900(config)# no access-list ACL1
Access List ACL1 was deleted.
OS900(config)#
```

# Example

Below is a configuration example showing the user inputs (in **bold**) and OS900 outputs on the CLI screen. The user inputs include:

- ACL creation
- Adding a comment (remark) on the ACL
- Creation of rules. Each rule consists of a criterion (condition) and the action for the rule
- Creation of an interface to which the ACL is to be applied
- Activation of the ACL using the command **access-group**.
- ACL status display
- Interface status display

```
OS900> enable
OS900# configure terminal
OS900(config)# access-list extended ACL1

OS900(config-access-list)# remark This ACL is for Sales Dept.

OS900(config-access-list)# rule 1
OS900(config-rule)# source-ip eq 10.10.10.10/32
OS900(config-rule)# action permit
OS900(config-rule)# exit

OS900(config-access-list)# rule
OS900(config-rule)# source-ip eq 4.4.4.4/32
OS900(config-rule)# action mirror-to-cpu
OS900(config-rule)# exit

OS900(config-access-list)# rule
OS900(config-rule)# source-ip eq 1.1.1.1/32
OS900(config-rule)# action mark sl 7
OS900(config-rule)# exit
OS900(config-access-list)# exit

OS900(config)# interface vlan vif2005
OS900(config-vif2005)# ports 2-4
OS900(config-vif2005)# tag 100
Interface is activated.
OS900(config-vif2005)# ip 193.88.88.234/24
OS900(config-vif2005)# access-group ACL1
OS900(config-vif2005)#

OS900(config-vif2005)# show access-group
Access List ACL1 is activated on inteface vif2005

OS900(config-vif2005)# show detail

vif2005 is DOWN (No state changes have occurred)
  Active: Yes
  Ports: 3-8
  Interface type is Vlan
  Encapsulation: 802.1Q,  Tag 100
  MAC address is 00:0F:BD:02:05:B8
  IP address is 193.88.88.234/24
  Cpu-membership is enable
  Management access is denied
  TFTP access is denied.
  Access-group is active:
      ACL1         Ports: all
OS900(config-vif2005)#
```

# Modifying an *Active* ACL

## General

An ACL that is active (bound) to one or more ports/VLANs can be modified *on-the-fly*, i.e., *while it is still bound*. Modifying an active ACL means one or more of the following:

– Adding a New Rule
– Deleting an Existing Rule
– Editing an Existing Rule

## Adding a New Rule

To add a new rule in an active ACL:

1. Enter the **access-list** mode of the ACL.
2. Create the new rule as described in the section *Creating a* Rule, page *297*, making sure that the index (ID) chosen for the new rule will position the rule among the other rules (if any) where required.
3. If the ACL has already been bound, to activate the new rule, in its **rule** mode invoke the command:
   **enable**

Example

```
OS900(config)# access-list extended test
OS900(config-access-list)# rule 15
OS900(config-rule)# source-ip eq 11.1.1.101/32
OS900(config-rule)# action list rate1
OS900(config-rule)# enable
OS900(config-rule)#
```

In the example above the new rule (Rule 15) is inserted between Rule 10 and Rule 20.

## Deleting an Existing Rule

To delete an existing or new rule:

1. Enter the **access-list** mode of the ACL containing the rule to be deleted.
2. Delete the rule by invoking the command:
   **no rule RULE_NUM**

   where,
   **RULE_NUM**: Index of the rule to be deleted

Example

```
OS900(config)# access-list extended test
OS900(config-access-list)# no rule 10
OS900(config-access-list)#
```

## Editing an Existing Rule

In editing an existing rule in an active ACL, Method 1 or 2 can be used.

### Method 1

In this method, the effect on the traffic while the rule is being edited is ignored.
To edit an existing rule in an active ACL:

1. Enter the **access-list** mode of the ACL containing the rule to be edited.
2. Enter the mode of the rule with the *old* index by invoking the command:
   **rule RULE_NUM**

   where,
   **RULE_NUM**: Old index of the rule to be edited

3. So that the rule can be edited, disable it by invoking the command:
   **`no enable`**
4. Edit the rule (having the new index) by invoking any one or more of the commands noted in the section *Creating a Rule*, page *297*, for classification and actions.
5. To activate the edited rule (having the old index), in its **`rule`** mode invoke the command:
   **`enable`**

<u>Example</u>

```
OS900(config)# access-list extended test
OS900(config-access-list)# rule 15
OS900(config-rule)# no enable
OS900(config-rule)# action list rate2
OS900(config-rule)# enable
OS900(config-access-list)#
```

**Method 2**

In this method, traffic is allowed to be forwarded unaffected while the rule is being edited.

To edit an existing rule in an active ACL:

1. Enter the **`access-list`** mode of the ACL containing the rule to be edited.
2. To allow traffic to be forwarded unaffected according to the *unedited* rule while the rule is being edited, copy the rule using a new index as follows:
   **`rule RULE_NUM copy RULE_NUM`**

   where,

   **`RULE_NUM`**: (First appearance) Old index of the rule to be edited

   **`RULE_NUM`**: (Second appearance) New index for the rule to be edited
3. Enter the mode of the rule with the *old* index by invoking the command:
   **`rule RULE_NUM`**

   where,

   **`RULE_NUM`**: Old index of the rule to be edited
4. So that the rule can be edited, disable it by invoking the command:
   **`no enable`**
5. Edit the rule (having the new index) by invoking any one or more of the commands noted in the section *Creating a Rule*, page *297*, for classification and actions.
6. To activate the edited rule (having the old index), in its **`rule`** mode invoke the command:
   **`enable`**
7. Exit to the **`access-list`** mode of the ACL containing the rule by invoking the command:
   **`quit`**
8. Delete the rule with the *new* index by invoking the command:
   **`no rule RULE_NUM`**

   where,

   **`RULE_NUM`**: New index of the rule to be edited

Example

```
OS900(config)# access-list extended test
OS900(config-access-list)# rule 15 copy 16
OS900(config-access-list)# rule 15
OS900(config-rule)# no enable
OS900(config-rule)# action list rate2
OS900(config-rule)# enable
OS900(config-rule)# quit
OS900(config-access-list)# no rule 16
OS900(config-access-list)#
```

## Example

The following example demonstrates how an active ACL can be modified *on-the-fly*.

----------------------------------------------------------------------An Active ACL----------------------------------------------------------------------

```
!
action-list rate1
 tc-action
  drop-red
  rate single-leaky-bucket cir 5m cbs 4K
!
action-list rate2
 tc-action
  drop-red
  rate single-leaky-bucket cir 3m cbs 4K
!
access-list extended test
 rule 10
  action list rate1
  dest-ip eq 11.1.1.10/32
!
interface vlan vif100
  tag 100
  ports 1-2
  access-group test
```

----------------------------------------------------------------Appending a New Rule----------------------------------------------------------------

```
OS900(config)# access-list extended test
OS900(config-access-list)# rule 20
OS900(config-rule)# source-ip eq 11.1.1.100/32
OS900(config-rule)# action permit
OS900(config-rule)# enable
```

The enable command above activates the new rule.

The resulting configuration is as follows:

```
access-list extended test
 rule 10
  action list rate
  dest-ip eq 11.1.1.10/32
 rule 20
  action permit
  source-ip eq 11.1.1.100/32
```

-----------------------------------------------------------------Inserting a New Rule-----------------------------------------------------------------

```
OS900(config)# access-list extended test
```

```
OS900(config-access-list)# rule 15
OS900(config-rule)# source-ip eq 11.1.1.101/32
OS900(config-rule)# action list rate1
OS900(config-rule)# enable
```

The resulting configuration is as follows:

```
access-list extended test
 rule 10
  action list rate1
  dest-ip eq 11.1.1.10/32
 rule 15
  action list rate1
  source-ip eq 11.1.1.101/32
 rule 20
  action permit
  source-ip eq 11.1.1.100/32
```

--------------------------------Editing an Existing Rule Ignoring its Effect on Traffic Flow--------------------------------

```
OS900(config)# access-list extended test
OS900(config-access-list)# rule 15
OS900(config-rule)# no enable
OS900(config-rule)# action list rate2
OS900(config-rule)# enable
```

Note that while rule 15 is disabled traffic from the source 11.1.1.101 is denied.

------------------------------------Editing an Existing Rule without Affecting Traffic Flow------------------------------------

```
OS900(config)# access-list extended test
OS900(config-access-list)# rule 15 copy 16
OS900(config-access-list)# rule 16
OS900(config-rule)# no enable
OS900(config-rule)# action list rate2
OS900(config-rule)# enable
OS900(config-rule)# quit
OS900(config-access-list)# no rule 15
OS900(config-access-list)# rule 16 move 15
```

Note that traffic from source 11.1.1.101 is forwarded according to rule 15, i.e., it is not denied, during the editing.

The resulting configuration is as follows:

```
access-list extended test
 rule 10
  action list rate1
  dest-ip eq 11.1.1.10/32
 rule 15
  action list rate2
  source-ip eq 11.1.1.101/32
 rule 20
  action permit
  source-ip eq 11.1.1.100/32
```

----------------------------------------------------------Deleting an Existing Rule----------------------------------------------------------

```
OS900(config)# access-list extended test
OS900(config-access-list)# no rule 10
```

The resulting configuration is as follows:

```
access-list extended test
 rule 15
  action list rate2
  source-ip eq 11.1.1.101/32
 rule 20
  action permit
  source-ip eq 11.1.1.100/32
```

# Counters

## General

There are 32 independent counters allocated for ACLs. Any counter may be assigned to any number of rules irrespective of whether they belong to the same or to differing ACLs. A counter is incremented for each packet whose attribute value(s) match those specified in the rule.

## Assignment

To assign a counter to an ACL rule:

1. Create/access the ACL (as described in the section *Creating/Accessing*, page *296*).
2. Enter the **rule** mode of the ACL.
3. Invoke the command:

   **action matching-counter-set <1-32>**

   where,

   **<1-32>**: Range of Counter IDs from which one is to be selected

Example

```
OS910(config-rule)# action matching-counter-set 4
OS910(config-rule)#
```

## Viewing

### Momentary Reading

#### *For All ACLs*

To view the *momentary* reading on a counter that shows the total count for *all ACLs* to which the counter is assigned:

1. Enter **enable** mode.
2. Invoke the command:

   **show access-list extended-matching-counter [<1-32>]**

   where,

   **[<1-32>]**: Range of Counter IDs from which one is to be selected. If no number is selected, all counters will be displayed.

Example

```
OS910# show access-list extended-matching-counter 4

 Counter  Matching-Packets         ACL          Rule  Active
==============================================================
     4             768      ACL1                  10    NO
                            ACL1                  20    NO
                            ACL2                  10    NO
                            ACL2                  30    NO
OS910#
```

Notice that in the above example, Counter 4 is assigned to rules 10 and 20 of ACL1 and to rules 10 and 30 of ACL2. The number of matching packets `768` is the total for these rules of ACL1 and ACL2.

### *For a Specific ACL*

To view the *momentary* reading on a counter that shows the total count for all rules of a *specific ACL* to which the counter is assigned:

To view the momentary reading of counters for a specific ACL:

1. Enter the mode of the ACL as described in the section *Creating/Accessing*, page *296*.
2. Invoke the command:

    **`show`**

<u>Example</u>

```
OS910(config-access-list)# show

Access List Extended ACL1
=========================
state: NOT ACTIVE
----------
Rule index: 10
 Action:
  Matching Counter ID 4, Matching Packets 309
  Deny
 Rule:
  Protocol: st
  Rule is enable.
----------
Rule index: 20
 Action:
  Matching Counter ID 4, Matching Packets 288
  Permit
 Rule:
  Rule is enable.
----------
default policy: deny all
OS910(config-access-list)#
```

Notice that in the above example, Counter 4 is assigned to rules 10 and 20 of ACL1. The number of matching packets just for rule 10 is `309` and just for rule 20 is `288`.

### *For a Specific Rule*

To view the *momentary* reading on a counter that shows the count for a *specific* rule to which the counter is assigned:

To view the momentary reading of the counter for a specific rule in an ACL:

1. Enter the mode of the ACL as described in the section *Creating/Accessing*, page *296*.
2. Enter the mode of the specific rule in the ACL by invoking the command:

    **`rule [RULE_NUM]`**

    where,

    **`[RULE_NUM]`**: Index of rule.
3. Invoke the command:

    **`show`**

Example

```
OS910(config-rule)# show
Rule index: 20
 Action:
  Matching Counter ID 4, Matching Packets 288
  Permit
 Rule:
  Rule is enable.
----------
OS910(config-rule)#
```

Notice that in the above example, Counter 4 is assigned to rule 20 of ACL1. The number of matching packets just for rule 20 is `288`.

**Continually Updated Reading**

***For All ACLs***

To view the *continually updated* (automatically refreshed) reading on a counter that shows the total count for *all ACLs* to which the counter is assigned:

1. Enter **enable** mode.
2. Invoke the command:

   **monitor access-list extended-matching-counter [<1-32>]**

   where,

   **<1-32>**: Range of Counter IDs from which one is to be selected. If no number is selected, all counters will be displayed.

***For a Specific ACL***

To view the *continually updated* reading on a counter that shows the total count for all rules of a *specific ACL* to which the counter is assigned:

1. Enter the mode of the ACL as described in the section *Creating/Accessing*, page *296*.
2. Invoke the command:

   **monitor**

***For a Specific Rule***

To view the *continually updated* reading on a counter that shows the count for a *specific* rule to which the counter is assigned:

1. Enter the mode of the ACL as described in the section *Creating/Accessing*, page *296*.
2. Enter the mode of the specific rule in the ACL by invoking the command:

   **rule [RULE_NUM]**

   where,

   **[RULE_NUM]**: Index of rule.
3. Invoke the command:

   **monitor**

## Removal

To remove a counter from an ACL rule:

1. Access the ACL (as described in the section *Creating/Accessing*, page *296*).
2. Enter the **rule** mode of the ACL.

   **no action matching-counter-set**

Example

```
OS910(config-rule)# no action matching-counter-set
OS910(config-rule)#
```

## Clearing

To clear one or all counters:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`clear access-list extended-matching-counter <1-32>|all`**

   where,

   **`<1-32>`**: Range of Counter IDs from which one is to be selected

   **`all`**: All counters

Example

```
OS910# clear access-list extended-matching-counter 4
OS910#
```

# Chapter 16: Software-based Access Lists (ACLs) for Layer 2 Protocols

## General

This chapter shows how to create and apply *software-based* Access Lists (ACLs) that handle *Layer 2 protocols*.

## Definition

A *software-based* ACL is a rule for handling *ingress Layer 2 protocol* traffic at each OS900 port. The rule consists of a set of packet *attribute values* (for the purpose of packet classification) and *actions* to be performed on packets that have these values.

Examples of attributes are: Protocol, Source physical port, and Packet VLAN tag.

Examples of actions are: Nest (Add) VLAN tag to packet and Mark[43] VPT.

## Applicability

An ACL can be applied to one or more s*pecific* ports (even if the ports are members of different VLAN interfaces)

## Number

Up to 50 ACLs (rules) can be created.

## Packet Speed

The ingress traffic speed at any port to which the ACL is applied must not exceed 50 pkts/sec.

## Configuring

### Port

To enable Layer 2 tunneling of protocols via ingress ports to which the ACL is to be applied:

```
port l2protocol-tunnel
(all|cdp|pvst+|stp|vtp|dtp|pagp|udld|lacp|lamp|efm|dot1x|elm
i|lldp|garp) PORTS-GROUP [drop]
```

where,

**`all`**: All protocol datagrams, i.e., **`cdp`**, **`pvst+`**, **`stp`**, and **`vtp`**

**`cdp`**: Cisco discovery protocol datagrams

**`pvst+`**: Cisco Per VLAN Spanning Tree Plus discovery protocol datagrams. (PVST+ provides the same functionality as PVST. PVST uses ISL trunking technology whereas PVST+ uses IEEE 802.1Q trunking technology.

PVST functionality is as follows:

It maintains a spanning tree instance for each VLAN configured in the network. It allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each

[43] Add the VPT in the packet if the packet does not have a VPT. Change the VPT in the packet.

VLAN as a separate network, it has the ability to load balance traffic (at OSI Layer 2) by enabling forwarding for some VLANs on one trunk and enabling forwarding for other VLANs on another trunk, without causing a Spanning Tree loop.

**stp**: IEEE 802.1w or IEEE 802.1s spanning-tree protocol datagrams

**vtp**: IEEE 802.3ad VLAN trunk protocol datagrams

**lamp**: Location Aware MAC Protocol

**efm**: Ethernet in the First Mile 802.3ah protocol

**dot1x**: Port Authentication IEEE 802.1x protocol

**elmi**: Ethernet Local Management Interface protocol

**lldp**: Link Layer Discovery Protocol

**garp**: GARP Multicast Registration Protocol

**PORTS-GROUP**: Group of ports to be configured as tunnel ports

**[drop]**: Drop packets

## ACL

An ACL is created in two stages:

Stage 1 – Packet Classification

Stage 2 – Actions on Packet

### Stage 1 – Packet Classification

Packet Classification is the specification of attribute values of packets (according to which the packets are to be forwarded or dropped). Examples of these attributes are: Protocol, Source physical port, and Packet VLAN tag.

To perform Stage 1 (packet classification):

1. Enter **configure terminal** mode
2. Invoke the command:

   **l2protocol-tunnel rule <1-50>**

   where,

   **<1-50>**: Index of rule (ACL).

   On creation of the rule, the **rule** mode is entered as indicated by the prompt `OS900(config-ruleX)#)`, where `X` designates the rule (ACL) number. The rule just created does *not* contain packet classification (or actions). To include packet classification in the rule, continue with the steps below.

   (To revoke the defined rule, invoke the command: **no l2protocol-tunnel rule**.)
3. Specify the source physical port (irrespective of whether the port is a member of a VLAN interface) by invoking the command:

   **src-phy-port eq PORT**

   where,

   **eq**: Equal to

   **PORT**: Physical port number

   (To revoke the source physical port classification, invoke the command **no src-phy-port**.)
4. Select the VLAN tag of the packet by invoking the command:

   **tag eq <0-4095>**

   where,

   **eq**: Equal to

   **<1-4095>**: VLAN tag of packet.

   (To revoke the VLAN tag classification, invoke the command **no tag**.)
5. [Optional] Select the protocol of the packets by invoking the command:

**protocol all|cdp|pvst+|stp|vtp**

where,

**all**: All protocol datagrams, i.e., **cdp**, **pvst+**, **stp**, and **vtp**

**cdp**: Cisco discovery protocol datagrams

**pvst+**: Cisco Per VLAN Spanning Tree Plus discovery protocol datagrams.

(PVST+ provides the same functionality as PVST. PVST uses ISL trunking technology whereas PVST+ uses IEEE 802.1Q trunking technology.

PVST functionality is as follows:

It maintains a spanning tree instance for each VLAN configured in the network. It allows a VLAN trunk to be forwarding for some VLANs while blocking for other VLANs. Since PVST treats each VLAN as a separate network, it has the ability to load balance traffic (at OSI Layer 2) by enabling forwarding for some VLANs on one trunk and enabling forwarding for other VLANs on another trunk, without causing a Spanning Tree loop.

**stp**: IEEE 802.1w or IEEE 802.1s spanning-tree protocol datagrams

**vtp**: IEEE 802.3ad VLAN trunk protocol datagrams

(To revoke the protocol classification, invoke the command **no protocol all|cdp|pvst+|stp|vtp [PORTS-GROUP]**.)

**Stage 2 – Actions on Packet**

Actions for a rule consist of selecting one or more actions (to be performed on a packet) conditional on the packet classification (Stage 1).

Stage 2 may be performed immediately after completing Stage 1, above, while in **rule** mode. **rule** mode is indicated by the prompt `OS900(config-ruleX)#`, where `X` designates the rule (ACL) number, and is applicable for the rule that is the instance (current).

To perform Stage 2 (Actions on Packet), select any *one* or more of the following actions, provided they do not conflict with one another:

1. Mark packets with a VPT value by invoking the command:

   **action mark vpt <0-7>**

   where,

   **mark**: Marking.

   **vpt**: VPT.

   **<0-7>**: Range of VPT values from which one can be selected. (If a VPT value already exists, it is overwritten.)

| | **Note** |
|---|---|
| | The VPT marking is effective only if the ingress port is *not* set as 'untagged' in port tag-outbound mode. For details, see section *Outbound Tag Mode*, page *137*. |

(To revoke VPT marking, invoke the command **no action mark vpt**.)

2. Nest a tag (add a higher level tag, e.g., an IEEE802.1ad q-in-q service provider bridge tag) to an incoming packet by invoking the command:

   **action tag nest <0-4095> [vpt <0-7>]**

   where,

   **<0-4095>**: Range of VLAN tags from which one tag is to be selected.

   **[vpt]**: (Optional) VLAN priority tag.

   **<0-7>**: Range of VLAN priority tags from which one tag is to be selected.

(To revoke tag nesting, invoke the command **no action tag nest**.)

3. [Optional] Redirect Layer 2 protocol packets to another group of ports by invoking the command:

   **`action redirect ports PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Group of ports to which Layer 2 protocol ingress packets are to be redirected. A packet will be redirected to one (or more) of these ports if the ports are members of the VLAN whose ID is the same as that of the packet tag. If none of the ports in this group is a member of such a VLAN, the packet will be dropped.

(To revoke redirection, invoke the command **`no action redirect ports [PORTS-GROUP]`**.)

## Example

```
OS904(config-rule1)# write terminal
Building configuration...

Current configuration:
! version os900-3-1-0-D29-06-09-1500
!
line vty
 exec-timeout global 13
!
port l2protocol-tunnel cdp 3
l2protocol-tunnel rule 1
 action mark vpt 5
 action tag nest 4022
 tag eq 207
 src-phy-port eq 3
 protocol cdp
!
OS904(config-rule1)#
```

# Deleting

To delete an ACL:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`no l2protocol-tunnel rule <1-50>`**

   where,

   **`<1-50>`**: Index of rule.

Example

```
OS904(config)# no l2protocol-tunnel rule 1
OS904(config)#
```

# Chapter 17: SNMP Management

## Requirements

For SNMP management of the OS900, you need to:

- Verify connectivity between the OS900 and the SNMP manager
- Enable SNMP management
- Configure SNMP parameters (e.g., SNMP NMS IP address, community names, etc.)

## Enabling

The procedure for enabling SNMP management is described in the section *Remote Management*, page *191*.

## Commands

All SNMP commands are accessible at the **`snmp`** mode.

To access **`snmp`** mode:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`snmp`**

## Management Functions

In **`snmp`** mode, CLI commands can be invoked to perform the following SNMP management functions:

– System Identification
– Access Control
– Trap Generation
– Display
– View-based Access Control Model (VACM)

## System Identification

The following system MIB objects can be set for the OS900:

***sysContact*** – Used to set contact information, e.g., about system administrator
***sysLocation*** – Used to set location information, e.g., about the OS900's location

To set the sysContact object, invoke the command:

**`contact ..`**

where,

`..:` Contact information text.

To set the sysLocation object, invoke the command:

**`location ..`**

where,

`..:` Location information text.

To view the sysContact and sysLocation objects, invoke the command:

**`show snmp system`**

Following is a configuration example:

```
MRV OptiSwitch 910 version d0907-21-07-05
OS900 login: admin
Password:
Last login: Thu Sep 1 01:26:19 2006 on ttyS0

OS900> enable
OS900# configure terminal
OS900(config)# snmp
OS900(config-snmp)# contact InternationalSupport@mrv.com
OS900(config-snmp)# location Paradise Island (P.O.B. 123)
OS900(config-snmp)# show snmp system
 location location Paradise Island (P.O.B. 123)
 contact InternationalSupport@mrv.com
OS900(config-snmp)#
```

# Access Control

The OS900 can be used to perform access control with the following SNMP versions:

- SNMP version 1/2c
- SNMP version 3

## SNMP Version 1/2c

### General

Access control in SNMPv1/2c is based both on Community String and on Source IP Address of the request.

### Community Strings

#### *Description*

Community strings (names) function like passwords. They are used to authenticate SNMP requests to monitor and/or configure the OS900. Each SNMP request packet that is received is checked for a community string, the associated access privilege, and the Source IP address of the request. Only if these present in the packet match those in the OS900 database, access is permitted. The same community string from different administrators can mean different access privileges (e.g., write-read, read-only, etc.), as can be seen in the examples that follow.

There are three access privileges:

- Write-read
- Read-only
- NotConfig

#### *Configuration*

*Write-read*

The write-read privilege permits the settings of the OS900 to be viewed and changed.

To set up a community string for the write-read privilege in the OS900 database, invoke the command:

**`community [1-10000000] write-read SOURCE COMMUNITY`**

where,

**`[1-10000000]`**: (optional) Index of the entry. This option can be used to define several community strings, modify an existing entry (by entering the same index and then the other attributes, e.g., access privilege, IP source, etc.), and to provide convenience in placing the entry in a specific position of order.

**`SOURCE`** can be:

**`default`**: Any Source IP address

**`localhost`**: From local host

**`A.B.C.D`**: Source IP address

**`A.B.C.D/M`**: Source IP prefix (address and mask)

**COMMUNITY**: Community string

*Read-only*

The read-only privilege permits the settings of the OS900 to be viewed only.

To set up a community string for the read-only privilege in the OS900 database, invoke the command:

**community [1-10000000] read-only SOURCE COMMUNITY**

where,

**[1-10000000]**: (optional) Index of the entry. This option can be used to define several community strings, modify an existing entry (by entering the same index and then the other attributes, e.g., access privilege, IP source, etc.), and to provide convenience in placing the entry in a specific position of order.

**SOURCE** can be:

**default**: Any Source IP address

**localhost**: From local host

**A.B.C.D**: Source IP address

**A.B.C.D/M**: Source IP prefix (address and mask)

**COMMUNITY**: Community string

*NotConfig*

The notConfig privilege permits viewing only the *basic* settings of the OS900, i.e., MIB-II System objects (mib-2 1) and SNMP objects (mib-2 11).

This enables users to verify whether the OS900 is alive and to draw the network-map from the OS900 without affecting its operation.

To set up a community string for the notConfig privilege in the OS900 database, invoke the command:

**community [1-10000000] notConfig SOURCE COMMUNITY**where,

**[1-10000000]:** (optional) Index of the entry. This option can be used to define several community strings, modify an existing entry (by entering the same index and then the other attributes, e.g., access privilege, IP source, etc.), and to provide convenience in placing the entry in a specific position of order.

**SOURCE** can be:

**default:** Any Source IP address

**A.B.C.D:** Source IP address

**A.B.C.D/M:** Source IP prefix (address and mask)

**localhost:** From local host

**COMMUNITY** is community string

To display the community object, invoke the command:

**show snmp community**

Below is an example for configuring *community strings* for the three access privileges *write-read*, *read-only*, and *notConfig*.

```
OS900> enable
OS900# configure terminal
OS900(config)# snmp
OS900(config-snmp)# community write-read 153.70.131.222 public
OS900(config-snmp)# community read-only 153.70.131.0/24 private
OS900(config-snmp)# community notConfig default public

OS900(config-snmp)# show snmp community

## User          Source             Community  Description
-- ------------- ------------------ ---------- --------------
10 write-read    153.70.131.222     public
20 read-only     153.70.131.0/24    private
30 notConfig     default            public
-- ------------- ------------------ ---------- --------------
```

```
OS900(config-snmp)#
```

| | **Note** |
|---|---|
| | If the same community string is assigned to two (or more) Source IP addresses belonging to the same subnet (even if different privileges are assigned to the Source IP addresses), an SNMP request will be processed *only* for the Source IP address entered first[44] using one of the **`community`** commands described above. Requests by the other Source IP address(es) will be ignored! |

The example below clarifies the note. It shows that the same community string, namely, **`public`** is assigned to two Source IP addresses belonging to the same subnet. The Source IP address entered first is `153.70.131.222`, as indicated by a lower index value, namely, 10 in the first column. As a result, SNMP requests from the source with this IP address will be processed. SNMP requests from the source with the IP address `153.70.131.0/24` will be ignored!

```
OS900(config-snmp)# community write-read 153.70.131.222 public
OS900(config-snmp)# community read-only 153.70.131.0/24 public
OS900(config-snmp)# community notConfig default public
OS900(config-snmp)# show snmp community

## User          Source             Community  Description
-- ------------- ------------------ ---------- --------------
10 write-read    153.70.131.222     public
20 read-only     153.70.131.0/24    public
30 notConfig     default            public
-- ------------- ------------------ ---------- --------------
OS900(config-snmp)#
```

***Deletion***

To delete a community string:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`snmp`**
3. Invoke the command
   **`no community INDEX`**
   where,
   **`INDEX:`** Index of the community entry. (The index of an entry can be viewed by invoking the command **`show snmp community`**.)

## SNMP Version 3

### General

Access control in SNMPv3 is based on two security passwords that can be defined for each of the access privileges (write-read, read-only, and notConfig) *by the user*.

- Authorization Password
- Privacy Password

The *Authorization* password entered by the user is encrypted in either **`MD5`** or **`SHA`** code (algorithm), per the user choice. In addition, the password can be hidden. The password must be at least 10 characters long.

---

[44] That is, with a lower index value in the display obtained when the command **`show snmp users`** is invoked (at the mode `snmp`).

The *Privacy* password is optional. If entered it is encrypted in **des** code. The password must be at least 10 characters long.

### Configuration

To set up the passwords in the OS900 database, invoke the command:

**user wruser|rouser|ncuser [8] md5|sha AUTHPASSWORD des|aes PRIVPASSWORD**where,

**wruser:** Write-read privileged user (can access all MIBs)

**rouser:** Read-only privileged user (can access all MIBs)

**ncuser:** Basic read-only privileged user (can access only system MIB)

**8**: (optional) Hides the authorization password

**md5**: MD5 code

**sha**: SHA code

**AUTHPASSWORD**: Authorization password

**des** DES privacy code

**aes** AES privacy code

**PRIVPASSWORD** Privacy password

### Viewing SNMP Configuration

To view the *SNMPv3* passwords configured by the user:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **snmp**
3. Invoke the command:
   **show snmp configuration**

### Viewing SNMP Users

To view the users that have been assigned *SNMPv3* passwords:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **snmp**
3. Invoke the command:
   **show snmp users**

Below is an example showing the user inputs, which include: *SNMPv3* passwords configuration for the access privilege write-read, SNMP configuration display command, and SNMP users display command.

```
OS900(config-snmp)# user wruser md5 ZorroTheFox des CondorBird
OS900(config-snmp)# show snmp configuration
!
! SNMP configuration
snmp
 contact InternationalSupport@mrv.com
 location Paradise Island (P.O.B. 123)
 community 10 write-read 153.70.131.222 public
 community 20 read-only 153.70.131.0/24 public
 community 30 notConfig default public
 user rouser 8 sha 0xfc2684ca3353ec5c29fb2788aa0005c38438e1b1
 user wruser 8 md5 0xd2a56a2972f6dd9719f5aa1bdf80cab5 des 0xac7aa70a22e2df6c2e74b8331
a41d5ec
!
OS900(config-snmp)# show snmp users
!
  ### userName     Auth Priv PublicString
  --- ------------ ---- ---- ------------
    1 rouser       sha  none
```

```
    2 wruser       md5  des
  --- ------------ ---- ---- ------------
OS900(config-snmp)#
```

# Trap Generation

## General

Traps are SNMP packets sent by the OS900 agent to one or more SNMP hosts (managers) when certain events external to the OS900 are detected or when the condition of the OS900 has changed significantly.

A trap may be a cold reset, a warm reset, detection of an interface link status change, an SNMP authentication failure due to an incorrect community string, or Dying Gasp (indication of time to failure due to power outage), etc.

The OS900 can be configured to send traps to several pre-specified IP destination addresses (trap hosts).

## Trap Host Specification

To specify what hosts are to receive traps:

1. Enter **configure terminal** mode.
2. Invoke either of the following commands:

   Command for SNMPv1/2

   **trapsess TARGET 1|2 COMMUNITY [inform]**

   where,

   **TARGET**: = Hostname (IP address or DNS name).

   **1**: SNMPv1 trap

   **2**: SNMPv2 trap

   **COMMUNITY**: = Community string

   **inform**: (optional) Get acknowledgement of receipt of trap from the host

   Command for SNMPv3

   **trapsess TARGET 3 wruser|rouser|ncuser [inform]**

   where,

   **TARGET**: = Hostname (IP address or DNS name).

   **3**: SNMPv3 trap

   **wruser**: Write-read privileged user (can access all MIBs)

   **rouser**: Read-only privileged user (can access all MIBs)

   **ncuser**: Basic read-only privileged user (can access only system MIB)

   **inform**: (optional) Get acknowledgement of receipt of trap from the host

## Trap Host Display

To display specification of trap hosts:

1. Enter **enable** mode.
2. Invoke the command:

   **show snmp traps**

## Enabling/Disabling Authentication Traps

To enable or disable sending of authentication traps to hosts:

1. Enter **snmp** mode.
2. Invoke the command:

   **authtrap enable|disable**

   where,

**enable**: Send authentication traps
**disable**: Do not send authentication traps

## Trap Host Deletion

To delete specification of a trap host:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no trapsess TARGET**

   where,
   **TARGET**: Hostname (IP address or DNS name).

Below is an example showing the user inputs (in **bold**) and OS900 outputs on the CLI screen. The user inputs include:

- Specification of trap hosts for SNMPv1, 2, and 3
- The command for displaying the specifications
- Deletion of the trap host 174.59.33.88, and
- The command for redisplaying the specifications

```
OS900(config-snmp)# trapsess 173.57.32.104 1 ZorroTheFox inform
OS900(config-snmp)# trapsess 174.59.33.88 2 LionTheKing inform
OS900(config-snmp)# trapsess 176.58.34.249 3 wruser inform
OS900(config-snmp)# show snmp traps
!
!trap HostName        Vers Community/User   IsInform    Privacy
!---- --------------- ---- ---------------- ------
 trap 173.57.32.104   1    ZorroTheFox        inform
 trap 174.59.33.88    2    LionTheKing        inform
 trap 176.58.34.249   3    wruser             inform
OS900(config-snmp)# no trapsess 174.59.33.88
OS900(config-snmp)# show snmp traps
!
!trap HostName        Vers Community/User   IsInform    Privacy
!---- --------------- ---- ---------------- ------
 trap 173.57.32.104   1    ZorroTheFox        inform
 trap 176.58.34.249   3    wruser             inform
OS900(config-snmp)#
```

## Trap Source Address Specification

To specify the **srcIP** (IP address of the OS900 interface via which traps are to be sent out):

1. Enter **configure terminal** mode.
2. Invoke the command:
   **source ip A.B.C.D**

   where,
   **A.B.C.D**: IP address of the OS900 interface via which traps are to be sent out.

Below is an example showing:

- User specification of the trap source IP address
- Display of the trap source IP address.

```
OS900(config-snmp)# source ip 195.86.224.1
OS900(config-snmp)# show snmp srcIP
 source ip 195.86.224.1
OS900(config-snmp)#
```

## Link Trap Type

### Custom

To cause the OS900 SNMP agent to send link traps of a user-specified type:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`snmp`**
3. Invoke the command:
   **`link-trap-parameters (all|cisco|ietf|legacy)`**

   where,

   **`all`**: Bind parameters: ifIndex, ifAdminStatus, ifOperStatus, ifDescr, ifType

   **`cisco`**: Bind parameters: ifIndex, ifDescr, ifType

   **`ietf`**: Bind parameters: ifIndex, ifAdminStatus, ifOperStatus

   **`legacy`**: Bind parameter ifIndex only (default)

```
OS900(config-snmp)# link-trap-parameters ietf
OS900(config-snmp)#
```

### Default

To cause the OS900 SNMP agent to send link traps of the default type (i.e., per the argument **`legacy`**), invoke the command **`no link-trap-parameters`** or **`default link-trap-parameters`**.

### Exclusion

To cause the OS900 SNMP agent to exclude one or more specific types of link trap, invoke the command **`no link-trap-parameters (all|cisco|ietf|legacy)`**.

## Alarms

Following are alarms per the osPORT.MIB sent by the OS900:

– Port is enabled by managemet (CLI or SNMP).

  Unlike the physical connection, this notification is dedicated exactly to reflect port enabling by the management commands.

– Port is disabled by managemet (CLI or SNMP).

  Unlike the physical disconnection, this notification is dedicated exactly to reflect port disabling by the management commands.

– SFP is inserted in a port (1 minute response time).

– SFP is removed from a port (1 minute response time).

# Viewing

To view SNMP information, invoke the command:

**`show snmp [all]|authtrapmode|community|engineID|objectID|srcIP|system|traps|users|configuration`**

where,

**`[all]`**: (optional) All SNMP information (default)

**`authtrapmode`**: Authentication traps mode (enabled or disabled)

**`community`**: Community objects

**`engineID`**: Engine ID. (Needed by SNMP-enabled devices in the datapath of SNMP traffic from a device.)

**`objectID`**: SNMP OID of OS900.

**`srcIP`**: IP address of VLAN interface in OS900 via which a trap was sent out.

**`system`**: MIB-II system data

**`traps`**: Trap hosts

**`users`**: SNMPv3 user privilege and encryption modes

**`configuration`**: = Run-time configuration

Example

```
OS900(config-snmp)# show snmp all
 SNMP Object ID: 1.3.6.1.4.1.629.22.1.1
 engineID 0x800007e503000fbd0005b8
## User          Source             Community  Description
-- ------------- ------------------ ---------- --------------
10 write-read    153.70.131.222     public
20 read-only     153.70.131.0/24    public
30 notConfig     default            public
-- ------------- ------------------ ---------- --------------
  ### userName     Auth Priv PublicString
  --- ------------ ---- ---- ------------
    1 wruser       md5  none
  --- ------------ ---- ---- ------------
!trap HostName        Vers Community/User   IsInform
!---- --------------- ---- ---------------- ------
 trap 173.57.32.104   1    ZorroTheFox        inform
 trap 176.58.34.249   3    wruser             inform
 authtrap enabled
OS900(config-snmp)#
```

# Deleting a User

To delete an SNMP user, invoke the command:

**`no user NAME|ncuser|rouser|wruser`**

where,

**`user`**: SNMPv3 secure user to be deleted
**`NAME`**: Secure name of any user
**`ncuser`**: Read-only user (only *system* MIB)
**`rouser`**: Read-only user (all MIBs)
**`wruser`**: Read-write user (all MIBs)

# View-based Access Control Model (VACM)

## General

The traditional SNMP method of controlling access to management information is based on so-called *community strings* (*names*). Each *community string* dictates the type of privilege (e.g., read-only, read-write, etc.) given to specific users accessing the SNMP agent. For example, the community string *`public`* may be defined to allow only read operations (GET and GETNEXT) while the community string *`private`* may be defined to allow both read and write operations (GET, GETNEXT, and SET).

These privileges are hard-coded (fixed) and when given they apply to *all* MIB trees present in the SNMP agent, i.e., it is not possible to restrict access by users to *subsets* of a MIB tree or even to *specific* MIB trees. To overcome this limitation, the VACM model per RFC 2575 is introduced.

The OS900 has both SNMP control capabilities: the simple traditional type as well as VACM.

## Definition

VACM is an SNMPv3 access-control security model based on views (readView, writeView, notifyView). These views are described in the section *Terminology*, page *342*.

## Purposes

VACM has two purposes:

1) To enable the administrator to restrict access by users to selectable subsets of MIB trees.

2) To provide security beyond the traditional community strings/names by imposing additional access restrictions, such as, IP source address, security name, etc. together with the *community string* type of restriction. Specifically it provides for verification:
   - That each received SNMP message has not been modified during its transmission through the network.
   - Of the identity of the user on whose behalf a received SNMP message claims to have been generated.

## Terminology

**securityLevel:** A security level identifies the level of security that will be assumed when checking access privileges (for members of a group). Different access privileges can be defined for different security levels.

The SNMP architecture recognizes three security levels:

*noAuth*: Provides lowest security (without authentication and without privacy).

*AuthNoPriv* Provides medium security (with authentication but without privacy).

*AuthPriv* Provides highest security (with authentication and with privacy).

**securityModel:** SNMPv1 (ID = 1), SNMPv2c (ID = 2), or user-based (ID = 3).

**securityName:** Human readable string representing a principal.

**groupName:** Name/ID of a group. A group is a set of zero or more <securityModel, securityName> tuples on whose behalf SNMP management objects can be accessed. A group defines the access rights afforded to all securityNames belonging to that group. The combination of a securityModel and a securityName maps to at most one group.

**readView:** The SNMP object *vacmAccess**Read**ViewName*. The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes *read* access.

**writeView:** The SNMP object *vacmAccess**Write**ViewName*. The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes *write* access.

**notifyView:** The SNMP object *vacmAccess**Notify**ViewName*. The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes access *for notifications*.

**Storage:** Whether for system or user storage. There are two storage units:

PERMANENT – System non-erasable storage

NONVOLATILE – User erasable storage

## Viewing Access Information

### System-Defined

To view the system-defined access information (privileges, etc.), invoke the command:

```
show snmp vacm permanent [group|access|view|all]
```

where,

`permanent`: Only permanent (system-defined) entries

`group`: Map (table) of a combination of securityName and securityModel into a groupName

`access`: Map of a groupName + securityLevel to MIB access

`view`: Map of a Views table

`all`: All VACM tables (default)

Example

```
OS900(config)# snmp
OS900(config-snmp)# show snmp vacm permanent

 ----------------------------------------Map of securityModel + securityName → groupName (user)----------------------------------------

securityModel securityName  groupName      Storage
------------- ------------- -------------- -------
         1    admin         RWGroup        PERMANENT
         1    initial       notConfigGroup PERMANENT
         1    notConfig     notConfigGroup PERMANENT
         1    read-only     ROGroup        PERMANENT
         1    write-read    RWGroup        PERMANENT
         2    admin         RWGroup        PERMANENT
         2    notConfig     notConfigGroup PERMANENT
         2    read-only     ROGroup        PERMANENT
         2    write-read    RWGroup        PERMANENT
         3    ncuser        notCfgGrpUSM   PERMANENT
         3    rouser        ROGrpUSM       PERMANENT
         3    wruser        RWGrpUSM       PERMANENT

 ---Map of groupName + securityModel → securityLevel + View Names (in columns readView, writeView, and notifyView)---

groupName      Model Level        readView   writeView  notifView  Storage
-------------- ----- ------------ ---------- ---------- ---------- -------
ROGroup        any   noauth       all        none       all        PERMANENT
RWGroup        any   noauth       all        all        all        PERMANENT
ROGrpUSM       3     authnopriv   all        none       all        PERMANENT
RWGrpUSM       3     authnopriv   all        all        all        PERMANENT
notCfgGrpUSM   3     authnopriv   systemview none       none       PERMANENT
notConfigGroup any   noauth       systemview none       none       PERMANENT

 --------------------------Map of View Names (all, systemview) → Views (Subtrees/subsets of MIB trees) --------------------------

Name          Incl/Excl Subtree                        Storage
------------- --------- ------------------------------ -------
all           include   iso                            PERMANENT
systemview    include   system                         PERMANENT
systemview    include   snmp                           PERMANENT
OS900(config-snmp)#
```

In the example above:

The *first* table [marked Map of securityModel + securityName → groupName (user)] shows the users (in column `securityName`) and the groups to which they belong (in column `groupName`). For e.g., the user `admin` belongs to the group `RWGroup`. Observe that the group `RWGroup` is available in `securityModel 1` (i.e., in SNMPv1) as well as in `securityModel 2` (i.e., in SNMPv2c).

The *second* table [marked Map of groupName + securityModel → securityLevel + View Names (in columns readView, writeView, and notifyView)] shows the views (*in* columns `readView`, `writeView`, and `notifView`) for each of the 3 types of access to the MIB tree (`readView`, `writeView`, and `notifView`) and the groups to which they belong (in column `groupName`). For e.g., the second line indicates that administrators belonging to group `RWGroup`, for `any` securityModel, have all 3 types of access to a MIB tree on the securityLevel `noauth`.

The *third* table marked [Map of View Names (all, systemview) → Views (Subtrees/subsets of MIB trees)] shows the possible views, namely, `all` and `systemview`. `all` (OID:=.1) includes all 3 types of access to a MIB tree. `systemview` includes the subtree `system` (OID:=.1.3.6.1.2.1.*1*) as well as the subtree `snmp` (OID:=.1.3.6.1.2.1.*11*).

Note that for the securityName `notConfig`, only the view `systemview` is accessible.

### User-Defined

To view the user-defined access information (privileges, etc.), invoke the command:

**show snmp vacm nonvolatile [group|access|view|all]**

where,

**nonvolatile**: Only non-volatile (user-defined) entries

**group**: Map of a combination of securityModel and securityName into a groupName

**access**: Map of a groupName to access

**view**: Views table

**all**: All VACM tables (default)

Example

```
OS900(config-snmp)# show snmp vacm nonvolatile

securityModel securityName  groupName      Storage
------------- ------------- -------------- -------
        1     Tarzan        JungleApes     NONVOLATILE

groupName      Model Level        readView   writeView  notifView  Storage
-------------- ----- ------------ ---------- ---------- ---------- -------
JungleApes     1     noauth       ApesRead   ApesWrite  ApesNotify NONVOLATILE

Name          Incl/Excl Subtree                       Storage
------------- --------- ----------------------------- -------
ApesRead      include   iso                           NONVOLATILE
ApesRead      exclude   rmon                          NONVOLATILE
ApesRead      exclude   nbSwitchG1                    NONVOLATILE
ApesWrite     include   system                        NONVOLATILE
ApesWrite     include   dot1dBridge                   NONVOLATILE
ApesWrite     include   ifMIBObjects                  NONVOLATILE
OS900(config-snmp)#
```

### All

To view the system-defined as well as the user-defined access information (privileges, etc.), invoke the command:

**show snmp vacm all [group|access|view|all]**

where,

**all**: (First appearance) Non-volatile as well as permanent entries

**group**: Map of a combination of securityModel and securityName into a groupName

**access**: Map of a groupName to access

**view**: Views table

**all**: (Second appearance) All VACM tables (default)

Example

```
OS900(config-snmp)# show snmp vacm all

securityModel securityName  groupName      Storage
------------- ------------- -------------- -------
         1    admin         RWGroup        PERMANENT
         1    Tarzan        JungleApes     NONVOLATILE
         1    initial       notConfigGroup PERMANENT
         1    notConfig     notConfigGroup PERMANENT
         1    read-only     ROGroup        PERMANENT
         1    write-read    RWGroup        PERMANENT
         2    admin         RWGroup        PERMANENT
         2    notConfig     notConfigGroup PERMANENT
         2    read-only     ROGroup        PERMANENT
         2    write-read    RWGroup        PERMANENT
         3    ncuser        notCfgGrpUSM   PERMANENT
         3    rouser        ROGrpUSM       PERMANENT
         3    wruser        RWGrpUSM       PERMANENT

groupName      Model Level        readView   writeView  notifView  Storage
-------------- ----- ------------ ---------- ---------- ---------- -------
ROGroup        any   noauth       all        none       all        PERMANENT
RWGroup        any   noauth       all        all        all        PERMANENT
ROGrpUSM       3     authnopriv   all        none       all        PERMANENT
RWGrpUSM       3     authnopriv   all        all        all        PERMANENT
JungleApes     1     noauth       ApesRead   ApesWrite  ApesNotify NONVOLATILE
notCfgGrpUSM   3     authnopriv   systemview none       none       PERMANENT
notConfigGroup any   noauth       systemview none       none       PERMANENT

Name          Incl/Excl Subtree                       Storage
------------- --------- ----------------------------- -------
all           include   iso                           PERMANENT
ApesRead      include   iso                           NONVOLATILE
ApesRead      exclude   rmon                          NONVOLATILE
ApesRead      exclude   nbSwitchG1                    NONVOLATILE
ApesWrite     include   system                        NONVOLATILE
ApesWrite     include   dot1dBridge                   NONVOLATILE
ApesWrite     include   ifMIBObjects                  NONVOLATILE
systemview    include   system                        PERMANENT
systemview    include   snmp                          PERMANENT
OS900(config-snmp)#
```

## Configuring a New User

VACM enables the administrator to configure new users (security names) that may include specific subtrees (subsets) of a MIB tree and exclude others.

The procedure consists of four stages as follows:

- Mapping Source Name + Community String → Security Name (user)
- Mapping Security Name + Security Model → Group Name
- Mapping Group Name + Security Model → Security Level + View Object *Names*
- Mapping View Object *Names* → Views (Subtrees/subsets of MIB trees)

Mapping Source Name + Community String → Security Name (user)

Invoke the command:

**community [<1-10000000>] (write-read|read-only|notConfig|NAME) (default|localhost|A.B.C.D|A.B.C.D/M) COMMUNITY**

where,

**<1-10000000>**: Number of Security Name

**write-read**: Security name providing write & read privileges to the whole MIB tree (OID:=.1)

**read-only**: Security name providing read-only privileges to the whole MIB tree (OID:=.1)

**notConfig**: Security name providing `systemview` privileges only, i.e., read-only privileges to the subtrees `system` (OID:=.1.3.6.1.2.1.1) and `snmp` (OID:=.1.3.6.1.2.1.11).

**NAME**: Security name (user) to be defined by the administrator

**default**: Source name representing all source IP addresses

**localhost**: Source name of local host, i.e., the OS900 at which a new Security name is being configured.

**A.B.C.D**: Source IP address

**A.B.C.D/M**: Source IP prefix (address and mask)

**COMMUNITY**: Community string

Example

```
OS900(config-snmp)# community Tarzan 192.2.2.2/24 private
OS900(config-snmp)#
```

Mapping Security Name + Security Model → Group Name

Invoke the command:

**vacm group (1|2|3) SECNAME GROUPNAME**

where,

**group**: Set entry in VACM group table

**1**: SNMPv1 Security Model

**2**: SNMPv2c Security Model

**3**: User-based Security Model (USM)

**SECNAME**: Security Name of the user (e.g., **Tarzan**)

**GROUPNAME**: Name of the group

Example

```
OS900(config-snmp)# vacm group 1 Tarzan JungleApes
user 'Tarzan' has been set to 'JungleApes' with security model 1
OS900(config-snmp)#
```

Mapping Group Name + Security Model → Security Level + View Object *Names*

Invoke the command:

**vacm access GROUPNAME (any|1|2|3) (noauth|authnopriv|authpriv) READVIEW WRITEVIEW NOTIFYVIEW**

where,

**access**: Set entry in VACM access table

**GROUPNAME**: Name of the group

**any**: All security Models (any)

**1**: SNMPv1 Security Model

**2**: SNMPv2c Security Model

**3**: User-Based Security Model (usm)

**noauth**: Low Security Level (without authentication and without privacy)

**authnopriv**: Medium Security Level (with authentication but without privacy)

**authpriv**: High Security Level (with authentication and with privacy)

**READVIEW**: Name of view for read access object.

**WRITEVIEW**: Name of view for write access object.

**NOTIFYVIEW**: Name of view for notifications object.

Example

```
OS900(config-snmp)# vacm access JungleApes 1 noauth ApesRead ApesWrite ApesNotify
OS900(config-snmp)#
```

Mapping View Object *Names* → Views (Subtrees/subsets of MIB trees)

Invoke the command:

**`vacm view NAME (include|exclude) MIBNODE`**

where,

**`view`**: Set entry in VACM view table

**`NAME`**: Name of the view object

**`include`**: Include the view (subtree) in the object

**`exclude`**: Exclude the subtree in the view

**`MIBNODE`**: objectID of the the view (subtree), for example, system or .7.1.3.6.1.2.1.1

Example

```
OS900(config-snmp)# vacm view ApesRead include .1
OS900(config-snmp)# vacm view ApesRead exclude nbSwitchG1
OS900(config-snmp)# vacm view ApesRead exclude RMON
OS900(config-snmp)# vacm view ApesWrite include system
OS900(config-snmp)# vacm view ApesWrite include ifMIBObjects
OS900(config-snmp)# vacm view ApesWrite include dot1dBridge
OS900(config-snmp)#
```

## Deleting an Entry from a VACM Table

### Group Table

To delete an entry from a VACM *group* table (see for instance the *first* table in the example in the section *System-Defined*, page *342*) invoke the command:

**`no vacm group 1|2|3 SECNAME [GROUPNAME]`**

where,

**`group`**: VACM group table from which an entry is to be deleted

**`1`**: SNMPv1 Security Model

**`2`**: SNMPv2c Security Model

**`3`**: SNMPv3

**`SECNAME`**: Security Name of the user

**`GROUPNAME`**: Name of the group

### Access Table

To delete an entry from a VACM *access* table (see for instance the *second* table in the example in the section *System-Defined*, page *342*), invoke the command:

**`no vacm access any|1|2|3 GROUPNAME noauth|authnopriv|authpriv`**

where,

**`access`**: VACM access table from which an entry is to be deleted

**`any`**: All security Models (any)

**`1`**: SNMPv1 Security Model

**`2`**: SNMPv2c Security Model

**`3`**: User-Based Security Model (USM)

**`GROUPNAME`**: Name of the group

**`noauth`**: Without authentication and without privacy

**`authnopriv`**: With authentication but without privacy

**`authpriv`**: With authentication and with privacy

### View Table

To delete an entry from a VACM *view* table (see for instance the *third* table in the example in the section *System-Defined*, page *342*), invoke the command:

**`no vacm view NAME include|exclude MIBNODE`**

where,

**`view`**: Delete entry from VACM view table

**`NAME`**: Name of the view

**`include`**: Include the subtree in the view

**`exclude`**: Exclude the subtree in the view

**`MIBNODE`**: objectID of the the subtree, for example, system or .7.1.3.6.1.2.1.1

## Configuration Example

The following example demonstrates the procedure for configuring VACM. It includes:

- The Source Name (IP prefix) **`192.2.2.2/24`** + Community String **`private`** mapping to the Security Name **`Tarzan`**
- The Security Name **`Tarzan`** + Security Model **`1`** (SNMPv1) mapping to the Group Name **`JungleApes`**
- The Group Name **`JungleApes`** + Security Model **`1`** mapping to the Security Level **`noauth`** + View Object Names **`ApesRead`**, **`ApesWrite`**, and **`ApesNotify`**
- The View Object Names **`ApesRead`**, **`ApesWrite`**, and **`ApesNotify`** mapping to the Views **`include .1`**, **`exclude nbSwitchG1`**, **`exclude RMON`**, **`include system`**, **`include ifMIBObjects`**, **`include dot1dBridge`**

```
OS900(config-snmp)# write terminal
Building configuration...

Current configuration:
! version 2_0_10
snmp

 community 10 Tarzan 192.2.2.0/24 private

 vacm group 1 Tarzan JungleApes

 vacm access JungleApes 1 noauth ApesRead ApesWrite ApesNotify

 vacm view ApesRead include iso
 vacm view ApesRead exclude rmon
 vacm view ApesRead exclude nbSwitchG1
 vacm view ApesWrite include system
 vacm view ApesWrite include dot1dBridge
 vacm view ApesWrite include ifMIBObjects
!
```

# Chapter 18: Port/VLAN Mirroring

## Terminology

*Ingress* port – A port at which traffic enters the OS900.

*Egress* port – A port at which traffic exits the OS900.

*Mirrored* port – A port whose traffic is replicated at another port/VLAN.

*Mirrored* VLAN – A VLAN whose traffic is replicated at another port/VLAN.

*Analyzer* port – A port at which traffic (received at another port/VLAN) is replicated.

*Analyzer* VLAN – A VLAN at which traffic (received at another port/VLAN) is replicated.

## Definition

Port/VLAN mirroring is the replication of traffic received on one or more physical ports (called *mirrored* ports) or at a VLAN interface (called *mirrored* VLAN) at another physical port (called *analyzer* or probe port) or at another VLAN interface (called *analyzer* VLAN).

## Purpose

Port/VLAN mirroring provides for the connection of a network protocol analyzer to an *analyzer* port/VLAN to identify the types of traffic passing through particular ports/VLANs. The data thus obtained can be used for statistical analyses to determine how to improve network operation as well as for troubleshooting a network on a port-by-port basis.

## Applicability

Mirroring can be applied to ingress, egress, or ingress & egress traffic received on one port, a group of ports, or at a VLAN. Instead of mirroring all traffic received at a port/VLAN, selective traffic, called a flow[45], at the port/VLAN can be mirrored. (To enable flow mirroring, an ACL must be bound to the port/VLAN. Configuration and binding of ACLs is described in ***Chapter 15:*** *Extended Access Lists (ACLs)*, page *295*.)

The packets can be mirrored to one analyzer port or to one analyzer VLAN. The advantage in selecting an analyzer VLAN is that an analyzer can be connected to a port of another switch in the network.

## Ingress Traffic Mirroring

In ingress traffic mirroring, the OS900 duplicates each packet that it *receives* at the port/VLAN to be mirrored. One of the duplicate packets is sent towards its destination and the other to the ingress analyzer port/VLAN.

Mirroring is ***not*** performed on ingress traffic that does not meet MAC level prerequisites. Accordingly, bad CRC packets, fragmented packets, etc. will not be mirrored.

All ingress packets pass through the ingress control pipe in the OS900. Some of these packets may be dropped or trapped to the CPU. In any case, such packets are forwarded to the analyzer port/VLAN.

---

[45] A flow is traffic at a port/VLAN that is definable with the following characterizations: destination address, source address, protocol, etc. – see *Stage 1 – Packet Classification*, page *297*.

# Egress Traffic Mirroring

In egress traffic mirroring, the OS900 duplicates each packet that it *transmits* from the port/VLAN to be mirrored. The egress mechanism is responsible for duplicating the packet. One of the duplicate packets is sent towards its destination and the other to the egress analyzer port/VLAN. The packet is mirrored only after verifying that there is no egress filtering to be applied to it and that it is not to be dropped on the egress transmit queues due to congestion.

# Analyzer Port/VLAN

Mirroring can be performed to one analyzer port or to one VLAN (that may have several member ports).

The speed of the analyzer port/VLAN is independent of the ingress and egress mirrored port(s)/VLAN speed. In some cases, the analyzer port/VLAN may be over-subscribed if the aggregate bandwidth of the mirrored traffic exceeds the analyzer port/VLAN link bandwidth. The congestion is handled in the same way as a regular transmit port congestion.

# Rules for Mirroring

1. One port, several ports, a VLAN, or a specific packet flow satisfying an ACL rule can be mirrored.
2. Only one port or one VLAN can be set as an analyzer port/VLAN.
   (This means that if any other port/VLAN is configured as an analyzer port/VLAN, the previous port/VLAN will cease to be an analyzer port/VLAN.)
3. The analyzer port/VLAN must be different from the mirrored port/VLAN.
4. The analyzer port must not be a trunk port.
5. The mirrored port and analyzer port may be of different bandwidth (e.g., 10 Mbps and 1000 Mbps) and/or different interface type (e.g., 100Base-TX and 100Base-FX). However, if the bandwidth of the analyzer port is smaller than that of the mirrored port, only part of the data traffic may be made available for analysis.

# Usage

## Analyzer Port

An analyzer port can be added, deleted, or viewed.

### Adding/Replacing Analyzer Port

To add an *analyzer port* or to replace it with a new one:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`port mirror to-analyzer port PORT`**
   where,
   **`PORT`**: Number of port to be an *analyzer port*.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# port mirror to-analyzer port 3
OS900(config)#
```

### Viewing Analyzer Port

To view the existing *analyzer port*, invoke the command **`show port mirror`**.

Example

```
OS900(config)# show port mirror
Ingress traffic is mirrored to analyzer port 3
Egress traffic is mirrored to analyzer port 3
```

```
OS900(config)#
```

### Deleting Analyzer Port

To delete the existing *analyzer port*, invoke the command:

**no port mirror to-analyzer**.

Example

```
OS900(config)# no port mirror to-analyzer
OS900(config)#
```

## Analyzer VLAN

An analyzer VLAN can be added, deleted, or viewed.

For the models OS912-AC-2 and OS912-DC-2, before adding or replacing an analyzer VLAN do the following:

1. Enter **configure terminal** mode and then **boot** mode
2. Invoke the command:
   **analyzer-vlan**
3. Exit to **enable** mode and reboot by invoking the command:
   **reboot**
   or
   **reboot-force**

> **Note**
> If an analyzer VLAN is configured on OS912-AC-2 or OS912-DC-2, *internal* Port 10 will become unavailable for all other operations requiring its use. For e.g., 'Rate limiting of flood packets for a *second* packet type at Port 10 – see **Chapter 10:** *Rate Limiting of Flood Packets*, page *249*', 'Ingress traffic shaping – see the section *Shaping*, page *375*', 'Tag translation/swapping – see **Chapter 12:** *Tag Translation/Swapping*, page *265*', and 'Binding a second ACL to a port – see the section *Binding*, page *316*.'

### Adding/Replacing Analyzer VLAN

To add an *analyzer VLAN* or to replace it with a new one:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **port mirror to-analyzer vlan <2-4093> vpt [<0-7>]**
   where,
   **<2-4093>**: Range of VLAN tags from which one is to be selected that represents the *analyzer VLAN*.
   **[<0-7>]**: New VLAN priority tag. The default is the original tag.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# port mirror to-analyzer vlan 3027 vpt 4
OS900(config)#
```

### Viewing Analyzer VLAN

To view the existing *analyzer* VLAN, invoke the command:

**show port mirror**

Example

```
OS900(config)# show port mirror
Ingress traffic is mirrored to analyzer vlan 3027 vpt 4
Egress traffic is mirrored to analyzer vlan 3027 vpt 4
```

```
OS900(config)#
```

#### Deleting Analyzer VLAN

To delete the existing *analyzer VLAN*, invoke the command:

**no port mirror to-analyzer**

Example

```
OS900(config)# no port mirror to-analyzer
OS900(config)#
```

## Mirrored Ingress Ports

One or more mirrored ingress ports can be added, deleted, or viewed.

#### Adding/Replacing Mirrored Ingress Ports

To add ports whose *ingress* traffic is to be mirrored or to replace them with new ones:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port mirror ingress PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports whose ingress traffic is to be *mirrored*.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# port mirror ingress 2-4
OS900(config)#
```

#### Viewing Mirrored Ingress Ports

To view the existing *mirrored ingress ports*, invoke the command:

**show port mirror**

Example

```
OS900(config)# show port mirror
Ingress traffic is mirrored from ports 2-4
OS900(config)#
```

#### Deleting Mirrored Ingress Ports

To delete the existing *mirrored ingress ports*, invoke the command:

**no port mirror**

Example

```
OS900(config)# no port mirror
OS900(config)#
```

## Mirrored Egress Ports

One or more mirrored egress ports can be added, deleted, or viewed.

#### Adding/Replacing Mirrored Egress Ports

To add ports whose *egress* traffic is to be mirrored or to replace them with new ones:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port mirror egress PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports whose egress traffic is to be *mirrored*.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# port mirror egress 1,2
OS900(config)#
```

### Viewing Mirrored Egress Ports

To view the existing *mirrored egress ports*, invoke the command:

**`show port mirror`**

Example

```
OS900(config)# show port mirror
Egress traffic is mirrored from ports 1-2
OS900(config)#
```

## Mirrored Ingress & Egress Ports

One or more mirrored ingress & egress ports can be added, deleted, or viewed.

### Adding/Replacing Mirrored Ingress & Egress Ports

To add ports whose *ingress & egress* traffic is to be mirrored or to replace them with new ones:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port mirror both PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Group of ports whose ingress & egress traffic is to be *mirrored*.

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# port mirror both 2-4
OS900(config)#
```

### Viewing Mirrored Ingress & Egress Ports

To view the existing *mirrored ingress & egress ports*, invoke the command:

**`show port mirror`**

Example

```
OS900(config)# show port mirror
Ingress traffic is mirrored from ports 2-4
Egress traffic is mirrored from ports 2-4
OS900(config)#
```

### Deleting Mirrored Ingress & Egress Ports

To delete the existing *mirrored ingress & egress ports*, invoke the command:

**`no port mirror`**

Example

```
OS900(config)# no port mirror
OS900(config)#
```

## Configuration

Any of a wide range of mirroring configurations can be implemented based on port ingress/egress traffic, VLAN, or ACL rule and destination port or VLAN. To cover this range and to serve as a guide that will enable the user to implement a configuration that best suits the purpose at hand, three configuration examples are presented below.

**Example 1**

This is a configuration in which traffic will be mirrored (from one or several ports) *to a single port*.

The configuration steps are as follows:

1. Add one analyzer port as described in the section *Adding/Replacing Analyzer Port*, page *350*.
2. Add one or more mirrored ports (whose ingress traffic, egress traffic, or both is to be mirrored) as described in any of the above sections, e.g., *Adding/Replacing Mirrored Ingress Ports*, page *352*.

Example

```
OS900# configure terminal

-----------------------------------------Adding one analyzer port-----------------------------------------

OS900(config)# port mirror to-analyzer port 1

-----------------------------------Adding one or more mirrored ports-----------------------------------

OS900(config)# port mirror both 2-4
OS900(config)#
```

**Example 2**

This is a configuration in which traffic will be mirrored (from one or several ports) *to a VLAN*.

The configuration steps are as follows:

1. Add one analyzer VLAN as described in the section *Adding/Replacing Analyzer Port*, page *350*.
2. Add one or more mirrored ports (whose ingress traffic, egress traffic, or both is to be mirrored) as described in any of the above sections, e.g., *Adding/Replacing Mirrored Ingress Ports*, page *352*.

Example

```
OS900# configure terminal

-----------------------------------------Adding one analyzer VLAN-----------------------------------------

OS900(config)# port mirror to-analyzer vlan 3027

-----------------------------------Adding one or more mirrored ports-----------------------------------

OS900(config)# port mirror both 2-4
OS900(config)#
```

**Example 3**

This is a configuration in which traffic in a *VLAN* will be mirrored (to a port).

The configuration steps are as follows:

1. Add one analyzer port as described in the section *Adding/Replacing Analyzer Port*, page *350*.
2. Select/create a mirrored VLAN (i.e., an interface whose traffic is to be mirrored. The procedure for creating/selecting an interface is described in ***Chapter 7:*** *Interfaces*, page *177*.)
3. Select VLAN Mode for the ports that are members in the mirrored VLAN.
4. Create an ACL that includes the rule that contains the action **`action mirror-to-analyzer`**.
5. Bind the ACL to the mirrored VLAN.

Example

```
OS900# configure terminal
```

-----------------------------------------Adding one analyzer port------------------------------------------

```
OS900(config)# port mirror to-analyzer port 1
```

---------------Selecting/creating a mirrored VLAN whose traffic is to be mirrored---------------

```
OS900(config)# interface vlan vif7
OS900(config-vif7)# ports 2-4
OS900(config-vif7)# tag 100
Interface is activated.
OS900(config-vif7)#
```

---------Selecting VLAN Mode for the ports that are members in the mirrored VLAN---------

```
OS900(config-vif7)# exit
OS900(config)# port acl-binding-mode by-vlan 2-4
OS900(config)#
```

------Creating an ACL that includes the rule action **`action mirror-to-analyzer`**------

```
OS900(config)# access-list extended ACL99
OS900(config-access-list)# rule
OS900(config-rule)# source-ip eq 2.2.2.2/32
OS900(config-rule)# action mirror-to-analyzer
OS900(config-rule)#
```

---------------------------------Binding the ACL to the mirrored VLAN---------------------------------

```
OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# interface vif7
OS900(config-vif7)# access-group ACL99
OS900(config-vif7)#
```

# **Chapter 19:** Traffic Conditioner

## Definition

Traffic Conditioner[46] (TC) is a set of functions for controlling the rate of ingress traffic of specific flows[47]. It complements the flow classification process described in ***Chapter 14:*** *Quality of Service (QoS)*, page *281.*

## Purpose

A TC is used to provide two key services related to aggregate flow:

- *SLA* enforcement: This service is implemented using metering, selective packet drop, and SL remarking
- Accounting *and billing*: For this service, flow aggregate counters are maintained

These two services are needed to limit ingress traffic and to account for it, typically at access points, such as, an Ethernet-to-Subscriber access box. By combining these services with ingress and egress traffic shaping (described in the section *Shaping*, page *375*), they form a complete SLA enforcement set of tools for service providers.

## Number

Up to 256 TCs can be configured on an OS900.

## Action List

### General

An Action List is a set of actions. Currently, a TC action is the only option in an Action List.

To activate a configured TC, its Action List must be included in an Access List (ACL) rule as described in the section *Stage 2 – Actions on Packet*, page *304*.

### Sharing

An Action List (e.g., TC) can be included in any number of ACL rules, which contain actions to be performed.

The advantage in applying one Action List to several ports/interfaces (i.e., using the Action List in sharing mode) becomes evident when the Action List has to be modified. In such an instance the Action List needs to be modified *just once* rather than several times, once for each port/interface.

### Creation/Access

To create/access an Action List:

1. Enter **`configure terminal`** mode
2. Invoke the command:

   **`action-list NAME`**

   where,

   **`NAME`**: Name of the Action List. (The name can be any string of alphanumeric characters.)

[46] Also known as policer, meter, or rate-limiter.

[47] A flow is streams of packets that comply with a specific ACL rule.

| | **Note** |
|---|---|
| | If an Action List already exists, it is enough to type the first few characters unique to its name and press Tab in order to access the Action List or complete its name. |

Example

```
OS900# configure terminal
OS900(config)# action-list ActionList1
OS900(config-action-list)#
```

## Viewing

### Status and Configuration

To view status and configuration information on an Action List:

1. Enter **enable** mode
2. Invoke the command:

   **show action-list [detail] [NAME|hidden]**

   where,

   **[detail]**: Details on the action list.

   **[NAME]**: Name of the action list. (The name can be any string of alphanumeric characters. If no name is entered, all the configured action lists are displayed.)

   **[hidden]**: Hidden action lists also.

Example

```
OS900# show action-list detail ACN1

action-list ACN1
================
Status: not active
Hw. index: 0
Number of actions: 1

TC
----
TC Hw.index: 0
Drop packets marked Red: enabled
Conformance counter set number is #3
Single Leaky Bucket parameters:
  cir=5m bits/sec, cbs=10K bytes,
OS900#
```

### Running Configuration

To view the configurations by CLI commands of all the Action Lists:

1. Enter **enable** mode
2. Invoke the command:

   **show running-config action-list**

Example

```
OS900# show running-config action-list
!
action-list ACN1
 tc-action
  drop-red
  counter-set-number 3
  rate single-leaky-bucket cir 5m cbs 10K
!
action-list ACN2
 tc-action
  counter-set-number 5
  rate single-leaky-bucket cir 13m cbs 400K
OS900#
```

# Functions

The TC can perform the following functions on ingress traffic:

- Metering
- Actions on Non-Conforming (Red) Traffic
    - Dropping or
    - SL Remarking according to CL
- Accounting

# Metering

## Model

Traffic metering is the process of measuring the time-based properties (e.g., rate) of a traffic stream. A TC may be configured to meter traffic flow according to the OS900's metering model, which is a single-rate 2-color marker.

The traffic flow rate is defined with the parameters Committed Information Rate (CIR) and Committed Burst Size (CBS) of the 'Leaky Bucket' mechanism. This mechanism can be likened to a water bucket having one hole, with CBS analogous to the bucket capacity and CIR analogous to the rate of water leakage through the hole. CIR can be set in kilobytes/sec, megabytes/sec, or gigabytes/sec units. CBS can be set in kilobytes or megabytes.

A packet is marked with the Conformance Level as follows:

- Green if it does not exceed the CIR and CBS
- Red otherwise

*Figure 39*, below, shows how the metering model handles a packet.

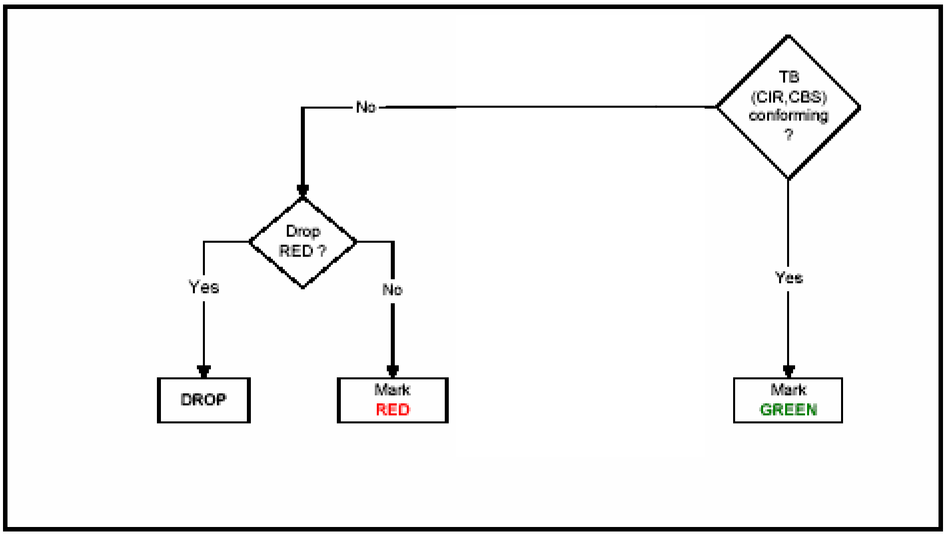



**Figure 39: Metering Operation**

Metering includes:

- Policing Mode
- Maximum Transmission Unit (MTU) for Policing
- Traffic Rate

## Policing Mode

### General

A policing mode is whether ingress traffic bytes counting is done to include the parts of Layer 1 frames, Layer 2 frames, or Layer 3 packets. Since a Layer 1 PDU $\supset$ Layer 2 PDU $\supset$ Layer 3 PDU, more bytes are counted for a Layer 1 PDU than for a Layer 2 PDU, and more bytes are counted for a Layer 2 PDU than for a Layer 3 PDU. The policing mode is global and applies for all TCs.

### Setting

To set the policing mode,

1. Enter **`configure terminal`** mode
2. Invoke the command:

    **`policing mode l1|l2|l3`**

    where,

    **`policing`**: Global policing.
    **`mode`**: Mode of policing.
    **`l1`**: Layer 1 bytes for counting.
    **`l2`**: Layer 2 bytes for counting. (Default)
    **`l3`**: Layer 3 bytes for counting.

Example

```
OS900(config)# policing mode l2
OS900(config)#
```

## Maximum Transmission Unit (MTU) for Policing

### General

If jumbo MTUs (longer than 2048 bytes) are to be forwarded in policing mode then, in addition to performing the setting for such MTUs as described in the section *Maximum Transmission Unit (MTU)*, page *115*, the setting as described in section *Custom* (just below) must also be performed. In both settings the MTUs must be at least as large as the jumbo MTUs required to be forwarded.

**Custom**

To set the MTU for policing:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **policing mtu (1536|2048|10240)**

   where,

   **1536**: MTU size 1536 bytes

   **2048**: MTU size 2048 bytes (default value)

   **10240**: MTU size 10240 bytes. Use this value for policer and jumbo frames

**Default**

To set the MTU for policing to the default value (2048 bytes):

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no policing mtu**

## Traffic Rate

To set the traffic rate:

1. Enter **configure terminal** mode.

   Example

```
OS900> enable
OS900# configure terminal
```

2. Create/access an Action List by invoking the following command.

   **action-list NAME**

   where,

   **NAME**: is the name of the action list. (The name can be any string of alphanumeric characters up to 20 characters long.)

   Example

```
OS900(config)# action-list ACN1
OS900(config-action-list)#
```

3. Enter the TC mode by invoking the command:

   **tc-action**

   Example

```
OS900(config-action-list)# tc-action
OS900(config-tc-action)#
```

4. Invoke the command:

   **rate single-leaky-bucket cir RATELIMIT cbs BURSTSIZE**

   where,

   **rate**: Traffic speed.

   **single-leaky-bucket**: Metering/marking algorithm whose coloring action depends on whether the **BURSTSIZE** (CBS) is exceeded. If it is not, a packet is colored green; otherwise it is colored red.

   **cir**: Committed Information Rate (CIR)

   **RATELIMIT**: CIR value. The value may be any number in the range 0-1G bits/sec. For OS930, the value may be any number in the range 0-10G bits/sec. Valid multiples are: **k** (= $10^3$), **m** (= $10^6$), or **g** (= $10^9$).. Examples of valid rates: **100k**, **10m**, **1g**.

   **cbs**: Committed Burst Size (CBS)

   **BURSTSIZE**: CBS value. This value is required to be larger than the policer MTU described in the section *Maximum Transmission Unit (MTU) for Policing*, page *360*. It is recommended to select a value that is greater than or equal to the size of the largest possible packet in the stream.

The value may be any number in the range 0-16M bytes. Valid units are: k, m. Examples: **`7k`**, **`2m`**.

(To allow any CIR rate, invoke the command **`no rate`**.)

# Actions on Non-Conforming (Red) Traffic

## General

Actions on non-conforming traffic include:

– Dropping
– SL remarking according to CL

## Dropping

Packets that do not conform with the limits specified by the metering model parameters CIR and CBS can be dropped.

To cause dropping for a specific TC:

1. Enter the Action List mode by invoking the command:
   **`action-list NAME`**
   where,
   **`NAME`**: Name of the action list. (The name can be any string of alphanumeric characters up to 20 characters long.)
2. Enter the TC mode by invoking the command:
   **`tc-action`**
3. Select dropping by invoking the command:
   **`drop-red`**

## SL Remarking According to CL

CL remarking is the changing of a packet SL based on its conformance level, i.e., color (red or green). It is always done. The CL is assigned to packets by the metering model of the TC. CL remarking overrides the SL assigned as described in ***Chapter 14:*** *Quality of Service (QoS)*, page *281* and the SL assigned as described in the section *Stage 2 – Actions on Packet*, page *304*.

Re-marking can be used for two purposes:

– To modify the internal forwarding priority within the egress queues.
– To modify the handling of a packet by downstream devices in the network.

## Default Map

To view the current CL remarking map, invoke the command **`do show cl-mapping`**.

*Table 15*, below, shows the default CL mapping.

**Table 15: Default CL Remarking Map**

| ORIG-SL | CL | NEW-SL |
|---|---|---|
| 1 | Red | 1 |
| 2 | Red | 2 |
| 3 | Red | 3 |
| 4 | Red | 4 |
| 5 | Red | 5 |
| 6 | Red | 6 |
| 7 | Red | 7 |
| 8 | Red | 8 |

## Custom Map

To change an existing CL remarking map:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

    **`cl-mapping orig-sl <1-8> red new-sl <1-8>`**

    where,

    **`<1-8>`**: (first) Range of SL values 1-8, from which one value is to be selected. The value is the SL marked as described in ***Chapter 14:*** *Quality of Service (QoS)*, page *281*.

    **`red`**: CL *red*

    **`<1-8>`**: (second) Range of SL values 1-8, from which one *new* value is to be selected.

    Example

```
OS900(config)# cl-mapping orig-sl 8 red new-sl 6
OS900(config)#
```

3. If required, repeat step *1*, above for other SL values.

## View Map

To view the existing CL remarking map:

1. Enter **`enable`** mode.
2. Invoke the command:

    **`show cl-mapping`**

    Example

```
OS900# show cl-mapping
ORIG-SL CL     NEW-SL
---------------------------------------------
1       red    1
2       red    2
3       red    3
4       red    4
5       red    5
6       red    6
7       red    7
8       red    6
OS900#
```

## Activation

For remarking to take effect, the metering model must be assigned to the Action List (using the command **`rate single-leaky-bucket cir RATELIMIT cbs BURSTSIZE`** as described in the subsection *Traffic Rate*, page *361*.)

## Deactivation

To deactivate remarking:

1. Enter **`configure terminal`** mode
2. Invoke the command:

    **`no cl-mapping orig-sl <1-8> red`**

    where,

    **`<1-8>`**: SL to be selected from the range 1 to 8

# Accounting Counters

## Number and Types

There are sixteen Global Counter Sets available for TCs. Each Global Counter Set consists of two counters. They are:

- Green CL byte Counter (Counts conforming bytes)
- Red CL byte Counter (Counts excess bytes)

## Size Adjustment

By default, each counter functions as a 32-bit counter. To set all counters to function as 64-bit counters:

1. Enter **`configure terminal`** mode
2. Invoke the command:
   **`tc-counters long-counters-mode`**

## Assignment & Activation

***One*** (or none) of these sixteen sets of counters may be assigned to each TC. . On assignment of a counter it is automatically activated. The procedure for assigning a counter set to a specific TC is as follows:

1. Enter **`configure terminal`** mode.

   Example
   ```
   OS900# configure terminal
   OS900(config)#
   ```
2. Enter the mode of the specific Action List by invoking the command.
   **`action-list NAME`**
   where,
   **`NAME`**: Name of the action list. (The name can be any string of alphanumeric characters up to 20 characters long.)

   Example
   ```
   OS900(config)# action-list ACN1
   OS900(config)#
   ```
3. Enter the TC mode by invoking the command:
   **`tc-action`**
4. Assign a global counter set by invoking the command:
   **`counter-set-number <1-16>`**
   where,
   **`<1-16>`**: Global counter sets 1 to 16 from which one is to be selected.

To replace a selected global counter set with another for a specific TC, invoke the **`counter-set-number <1-16>`** using the new global counter set number instead of **`<1-16>`**.

To dissociate a selected global counter set from a specific TC, invoke the **`no counter-set-number`**.

Each counter shows the aggregate of counts for all the TCs assigned to the counter.

The counters may count either the entire Layer 1 packet bytes (including inter-packet gap and preamble) or just the Layer 2 packet bytes. Section *Policing Mode*, page *360*, shows how to set the counting mode.

Global Counter Sets are used for statistical analyses and troubleshooting.

## Viewing

### Method 1

To view the counter readings for a specific TC in TC mode:

1. Enter the TC mode as described in the section *Activation*, page *363*.
2. To display counter readings *with* refresh (continual update), invoke the command:
   **`monitor tc-counters`**
3. To display counter readings *without* refresh, invoke the command:
   **`show tc-counters`**

Example

```
OS900# configure terminal
OS900(config)# action-list ACN1
OS900(config-action-list)# tc-action
OS900(config-tc-action)# show tc-counters

TC Conformance Counter Set#1:
--------------------------------
         1478934 - Number of bytes marked green
         381 - Number of bytes marked red
OS900(config-tc-action)#
```

### Method 2

To view the counter readings for a specific TC from **`enable`** mode:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show tc-counters AL_NAME`**
   where,
   **`AL_NAME`**: Name of the action list. (The name can be any string of alphanumeric characters up to 20 characters long.)

## Clearance

To clear the Specific Counter Set of a TC:

1. Enter the TC mode as described in the section *Activation*, page *363*.
2. Invoke the command:
   **`clear tc-counters`**

Example

```
OS900# configure terminal
OS900(config)# action-list ACN1
OS900(config-action-list)# tc-action
OS900(config-tc-action)# clear tc-counters
```

## Aggregation

### Configuration

Accounting for several existing TCs (assigned using action lists) can be unified as follows:

1. Enter **`configure terminal`** mode.
2. To enter the **`tc-counters-group`** mode, invoke the command:
   **`tc-counters-group NAME`**
   where,
   **`NAME`**: Name for the group of existing TCs whose accounts are to be unified.
   (To cancel aggregate accounting, invoke the command **`no tc-counters-group NAME`**.)
3. To provide a textual description for the group of TCs, invoke the command:
   **`description TEXT`**
   where,
   **`TEXT`**: Textual description for the group.

(To delete the textual description for the group of TCs, invoke the command **`no description`**.)

4. To include an existing TC in the joint accounting, invoke the command:
   **`action-list NAME`**
   where,
   **`NAME`**: Name for the action list assigned to the existing TC whose account is to be unified with those of other TCs.

   (To delete the action list, invoke the command **`no action-list NAME`**.)
5. Repeat the above step for each action list assigned to an existing TC whose account is to be unified with those of other TCs.

Example

```
OS900# configure terminal
OS900(config)# tc-counters-group ?
  NAME  Name of the group
OS900(config)# tc-counters-group WaterPark
OS900(config-tc_group-WaterPark)# description Customers are C118, C119, C120.
OS900(config-tc_group-WaterPark)# action-list ACN1
OS900(config-tc_group-WaterPark)# action-list ACN2
OS900(config-tc_group-WaterPark)#
```

### Viewing

#### *Groups*

To view configured groups of Action Lists:

1. Enter **`enable`** mode.
2. Invoke either of the following commands:
   **`show tc-counters-group [configuration]`**

Example

```
OS900> enable
OS900# show tc-counters-group configuration
!
! TCGROUP configuration
!
tc-counters-group JurassicPark
 action-list ACN3
!
tc-counters-group WaterPark
 action-list ACN1
 action-list ACN2
!
OS900#
```

#### *Aggregate Counts*

Method 1

To view the aggregate counts of a specific group of TCs, whose accounting has been unified, in **`tc-counters-group`** mode:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`tc-counters-group NAME`**
   where,
   **`NAME`**: Name for the group of TCs whose accounts have been unified.
3. Invoke either of the following commands:
   **`show`**
   **`monitor`**
   where,
   **`show`**: Display *without* refresh.
   **`monitor`**: Display *with* refresh.

Example

```
OS900# configure terminal
OS900(config)# tc-counters-group WaterPark
OS900(config-tc_group-WaterPark)# show
Traffic conditioner counters groups:
Flags: a - absent; i - inactive; m - metering;
       <1-16> - conformance counter set number

Group:WaterPark
Action-list  |Flags| Bytes Green | Bytes   Red |
ACN1         i             78905            0
ACN2         i           8063942            0
summary:                        0            0

OS900(config-tc_group-WaterPark)#
```

Method 2

To view the aggregate counts of the group of TCs, whose accounting has been unified, in **enable** mode:

1. Enter **enable** mode.
2. Invoke either of the following commands:

    **show tc-counters-group [NAME]**

    **monitor tc-counters-group [NAME]**

    where,

    **show**: Display *without* refresh.

    **monitor**: Display *with* refresh.

    **NAME**: Name of the group of TCs whose accounts have been unified.

Example

```
OS900> enable
OS900# show tc-counters-group configuration
!
! TCGROUP configuration
!
tc-counters-group JurassicPark
 action-list ACN3
!
tc-counters-group WaterPark
 action-list ACN1
 action-list ACN2
!
OS900#
```

# Activation

To activate a configured TC, include its Action List in an ACL rule as described in the section *Stage 2 – Actions on Packet*, page *304*.

# Dual Leaky-Bucket Policer

## General

A dual leaky-bucket policer can be configured using two single leaky buckets sequentially.

In some applications it is required to define a dual leaky-bucket policer, e.g., a trTcm (2-rate 3-color meter, as defined in RFC 2698). In the following example we show how such a policer can be implemented using two single-leaky-bucket policers run sequentially.

Assuming we want to implement a trTcm defined by a CIR, CBS, PIR, and PBS (peak burst size).

We use two TCs. The first is defined by the larger bucket (PIR, PBS) and the second is defined by the smaller bucket (CIR, CBS). The first TC will be configured to drop red packets. The second TC will not drop red traffic but will mark it as red (as having higher drop precedence). In this way, traffic not conforming with PIR/PBS will be dropped. Traffic conforming with PIR/PBS and not conforming with CIR/CBS will be marked red on the second TC (this is the equivalent for yellow traffic in the first TC), and traffic conforming with both will be marked green by the second TC.

## Configuration

The configuration steps are:

1. Define two TCs: One for the bigger bucket (PIR, PBS) and the second for the smaller bucket (CIR, CBS). (Note that a TC may be called 'smaller' if either the burst-size or the rate or both are smaller).
2. Define two ACLs, one for each TC.
3. Set the ingress port (port 1) to **by-port** ACL binding mode
4. Bind the ACL with the bigger TC to the port.
5. Bind the ACL with the smaller TC to the port as **extra** (second ACL for the port).

Example

In the example below the PIR is 10 Mbps, the PBS is 100 KB, the CIR is 2 Mbps, and the CBS is 100 KB.

```
OS900> enable
OS900# configure terminal
OS900(config)# action-list pirpbs
OS900(config-action-list)# tc-action
OS900(config-tc-action)# rate single-leaky-bucket cir 10m cbs 100k
OS900(config-tc-action)# drop-red
OS900(config-tc-action)# counter-set-number 1

OS900(config-tc-action)# exit
OS900(config-action-list)# exit
OS900(config)# action-list circbs
OS900(config-action-list)# tc-action
OS900(config-tc-action)# rate single-leaky-bucket cir 2m cbs 100k
OS900(config-tc-action)# counter-set-number 2

OS900(config-tc-action)# exit
OS900(config-action-list)# exit
OS900(config)# access-list extended pirpbs
OS900(config-access-list)# rule 10
OS900(config-rule)# action list pirpbs
OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# access-list extended circbs
OS900(config-access-list)# rule 10
OS900(config-rule)# action list circbs

OS900(config-rule)# exit
OS900(config-access-list)# exit
OS900(config)# port acl-binding-mode by-port 1
OS900(config)# port access-group pirpbs 1
OS900(config)# port access-group extra circbs 1
OS900(config)#
```

**Notes**

1. In the above example, the trTcm red bytes counter can be viewed by viewing the red bytes counter of counter-set 1, the trTcm yellow bytes counter can be viewed by viewing the red bytes counter in counter-set 2, and the trTcm green bytes counter can be viewed by viewing the green bytes counter in counter-set 2.
2. For implementing an srTcm (RFC 2697) a similar method can be applied: the CIR will be the rate of both TCs, the EBS will be the burst size of the first (bigger) TC and the CBS will be the burst size of the second (smaller) TC.

# Chapter 20: Egress-Queue Manager (EQM)

## Definition

The Egress Queue Manager (EQM) is used to provide traffic control and monitoring services on outbound traffic queues.

## Purpose

The purpose of the EQM is to perform the following functions at each physical port:

- Prevent congestion in queues
- Ensure that at least the minimum bandwidth allocated to each queue is provided
- Limit rate to the allocated bandwidth and shape individual queues
- Schedule flows from multiple queues

## Global Configuration

The EQM can provide a shared resource (common memory space) for buffering packets that may not be immediately forwarded at their port/queue due to the fact that the buffer space allocated to the port/queue is limited.

## Port Configuration

The EQM maintains the following per egress port:

- Maximum egress rate set for the port for Token Bucket shaping, in addition to the per-queue shaping. (This is useful for limiting the egress bandwidth for each port.)
- Scheduling modes (SP, WRR1, WRR0) for the port's queues – see the section *Scheduling*, page *372*, for details.

## Queue Configuration

The EQM maintains the following configuration parameters per queue per egress port:

- Queue enable/disable
- Maximum number of packet buffers and descriptors allowed for the queue, i.e., a per queue per drop-precedence configuration. (This constraint prevents a congested port/queue from using up all egress buffer and descriptor space in the OS900.)
- Queue shaping parameters, i.e., shaping Token Bucket profile. (This is useful for limiting the egress bandwidth for each queue.)
- Weight for WRR scheduler (if the queue is scheduled according to WRR)

## Congestion Avoidance

Congestion is a condition in which the OS900 is unable to receive and process all packets arriving at its ports. It can occur when:

- The data speed on the transmission link remains smaller than the data speed on the reception links over a period of time. Examples of situations that may lead to such congestion are:

   1. A Gigabit port transmits more than 100Mbps to a Fast Ethernet port.
   2. A Gigabit port transmits at a high bandwidth to a Gigabit port configured to perform egress shaping (described in the section *Shaping*, page *375*.)
   3. Several Gigabit ports transmit to one Gigabit port at a total rate that exceeds 1Gbps.
- The bandwidth provided for a low(er) priority queue is too small
- Flow Control is activated by a device at the other end of the transmission link

This problem is resolved by the OS900 using the congestion avoidance mechanism called Tail-Drop.

# Scheduling

## General

Scheduling is the process of selecting packets from egress queues for placement on a transmission link. Scheduling depends on the scheduling mode (described below) and QoS factors such as traffic shaping (described in the section *Shaping*, page *375*).

## Scheduling Modes

There are three scheduling modes for queues. They are:

– Strict Priority (SP)
– Shape-deficit Weighted Round Robin 1 (WRR1)
– Shape-deficit Weighted Round Robin 0 (WRR0)

The general relationship between the modes is as follows:

Queues assigned to SP mode are scheduled before queues assigned to WRR1 mode and WRR0 mode.

If queues are assigned to WRR0 mode and WRR1 mode, the highest of these queues will cause the queues of the mode to which it is assigned to be scheduled before the queues of the other mode. For example, suppose queues 2, 3 and 6 are assigned to WRR1 and queues 4 and 7 are assigned to WRR0. Since the highest of these queues is 7 and it is assigned to WRR0, queues 4 and 7 will be scheduled before queues 2, 3, and 6.

Assignment of queues (SLs) to WRR0 and WRR1 queues is done with the command **`priority-queuing sl <1-8> wrr0|wrr1 weight <1-255> profile <1-7>`**, described in the section *Priority Queuing*, page *373*.

The user can set each queue at each port in any one of the scheduling modes.

The user can also set a further relationship between these modes such as rate limit per queue as described in the section *Shaping*, page *375*.

The general relationship between the modes, the capability to set a queue in any one of the modes, and the capability to set a rate limit per queue enables support for high level QoS applications (e.g., the IETF DiffServ standardized PHBs such as Assured Forwarding (AF), Expedited Forwarding (EF), Best Effort, etc.).

Scheduling queues in both SP and WRR modes enables handling of highly time-sensitive traffic (such as VoIP and mission critical protocols) and other traffic on the same link bandwidth.

### Strict Priority (SP)

A queue assigned to SP queue has *higher* scheduling priority than a queue assigned to WRR1 or WRR0 queue, even if it assigned a lower SL.

At each port, a queue in SP mode that has higher SL[48] is scheduled before queues in SP mode that have lower SL. Accordingly, if, for e.g., queues 6 to 8 are in SP mode, queue 8 (SL8) is scheduled before queue 7 (SL7), and queue 7 before queue 6.

[48] SL is DiffServ Service Level or Class of Service (CoS). SL can have any value from 1 to 8.

This means the following:

- The egress port serves queue 8 as long as packets are waiting in that queue, and lower queues are served only when queue 8 is empty.
- If queue 8 is empty, the egress port serves queue 7 as long as packets are waiting in that queue, and lower queues are served only when queue 7 is empty.

#### Weighted Round Robin 1 (WRR1)

At each port, queues in WRR1 mode share the available link bandwidth in proportion to the weights assigned to them. The weights can have any value in the range 1 and 255 so that the weight ratio of two queues in WRR1 mode can be as high as 255:1. If a weight **W** is assigned to a queue **W x 256** bytes will be transmitted from the queue before transmission begins from another queue.

This above description of WRR operation is roughly correct. The actual operation is more complex and resembles the WFQ scheduling algorithm that provides fairness among the various WRR queues.

Accordingly, weight 1 is equivalent to 256 bytes, weight 2 is equivalent to 2 x 256 bytes, etc., so that weight 255 is 63.75 Kbytes. As a result, the distribution of bandwidth among queues in a WRR group will be directly proportional to the weights.

#### Weighted Round Robin 0 (WRR0)

The description given for WRR1 in the section just above applies for WRR0 just as well.

## Configuration

### General

This section shows how to configure scheduling for each queue by setting it into one of the three modes and assigning to the queue a weight if it is set in WRR1 or WRR0 mode.

### Priority Queuing

To avoid confusion, ensure that:

- Queues in SP mode have higher SL values than queues in WRR1 mode and WRR0 mode, and
- Queues in WRR1 mode have higher SL values than queues in WRR0 mode.

For example, queue 6 should not be set in SP if queue 7 is set in WRR1.

Setting all queues in SP mode without traffic shaping or ingress rate limiting (policing) may prevent progress of lower SL queues.

The default weights for the eight queues in WRR1 or WRR0 mode are as follows:

| **Queue** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| **Weight** | 1 (= 256 bytes) | 16 (= 4K bytes) | 32 (= 8K bytes) | 48 (= 12K bytes) | 64 (= 16K bytes) | 80 (= 20K bytes) | 96 (= 24K bytes) | 112 (= 28K bytes) |

To assign queues[49] to modes (SP, WRR0, WRR1):

1. Enter **`configure terminal`** mode.
2. For WRR0 or WRR1, invoke the command:

```
priority-queuing sl <1-8> wrr0|wrr1 weight <1-255> profile <1-
7>
```

where,

**`<1-8>`**: Number of Service Level

**`wrr0`**: WRR0 mode

**`wrr1`**: WRR1 mode

**`<1-255>`**: WRR weight value in units of 256 bytes

[49] A queue is identified by SL. Thus, queue 1 is SL 1, queue 2 is SL 2, etc.

**<1-7>**: Profile number

3. For SP or default, invoke the command:

   **`priority-queuing sl <1-8> sp|default profile <1-7>`**

   where,

   **<1-8>**: Number of Service Level

   **sp**: SP mode

   **default**: Assign the queue (SL) to SP mode

   **<1-7>**: Profile number

### Profiles

Up to 7 global profiles can be defined for ports using the **`port priority-queuing profile`** command. To each port one profile can be assigned to ingress traffic and one to egress traffic. If the port is a trunk *only one and the same* profile can be assigned to the member ports of the trunk.

To assign a profile to *egress* traffic at a port/group:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port priority-queuing profile <1-7> [PORTS-GROUP]`**

   where,

   **[PORTS-GROUP]**: Group of Ports

To assign a profile to *ingress* traffic at a port/group:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`port priority-queuing profile <1-7> ingress [PORTS-GROUP]`**

   where,

   **[PORTS-GROUP]**: Group of Ports

By default, all ports are assigned to profile 1.

### Example

The example below demonstrates how to configure scheduling. Suppose the scheduling conditions are as follows: :

- Applicability to ports 3 and 4.
- Queues 6 to 8 in SP
- Queues 3 to 5 in WRR1
- Queues 3, 4, and 5 have 5 Kbytes (weight 20), 7.5 Kbytes (weight 30), and 15 Kbytes (weight 60), respectively of the bandwidth for WRR1
- Queues 1 and 2 in WRR0
- Queues 1 and 2 have 10 Kbytes (weight 40) and 12.5 Kbytes (weight 50), respectively of the bandwidth for WRR0

Packets entering queues 6 to 8 will be forwarded first. Packets entering queues 3 to 5 will be forwarded provided the queues 6 to 8 are empty. Packets entering queues 1 and 2 will be forwarded provided the queues 3 to 8 are empty. Packets in queue 7 will be forwarded provided queue 8 is empty. Packets in queue 6 will be forwarded provided queues 7 and 8 are empty.

```
OS900> enable
OS900# configure terminal
OS900(config)# priority-queuing sl 8 sp profile 2
OS900(config)# priority-queuing sl 7 sp profile 2
OS900(config)# priority-queuing sl 6 sp profile 2
OS900(config)# priority-queuing sl 5 wrr1 weight 60 profile 2
Set weight 60 (15k bytes)
OS900(config)# priority-queuing sl 4 wrr1 weight 30 profile 2
Set weight 30 (7.5k bytes)
OS900(config)# priority-queuing sl 3 wrr1 weight 20 profile 2
Set weight 20 (5k bytes)
OS900(config)# priority-queuing sl 2 wrr0 weight 50 profile 2
```

```
Set weight 50 (12.5k bytes)
OS900(config)# priority-queuing sl 1 wrr0 weight 40 profile 2
Set weight 40 (10k bytes)
OS900(config)# port priority-queuing profile 2 3,4
port 3 scheduler profile set to: 2
port 4 scheduler profile set to: 2
OS900(config)#
```

### Viewing

To view a configured Flow Scheduler, invoke the command:

**`show priority-queuing profile <1-7>`**

where,

**`show`**: Display information.

**`priority-queuing`**: Queuing priority in respect to queues.

**`profile`**: Scheduler profile.

**`<1-7>`**: Profile number.

```
OS900(config)# show priority-queuing profile 2

PRIORITY-QUEUING
======================
SL   GROUP     WRR-WEIGHT
---------------------------
Profile 2  Port Members:3-4
-------------------------
1    wrr0      40  (10K)
2    wrr0      50  (12.5K)
3    wrr1      20  (5K)
4    wrr1      30  (7.5K)
5    wrr1      60  (15K)
6    sp        -
7    sp        -
8    sp        -
OS900(config)#
```

# Shaping

### General

Shaping is a mechanism for regulating traffic (ingress traffic at dual ports or egress traffic) in order to smoothen traffic flow.

Shaping can be used to limit and shape the traffic rate for specific egress queues or for the whole egress port.

Traffic rate per queue is limited by the per-queue Token Bucket mechanism. Traffic that is in-profile with the Token Bucket parameters is transmitted on the link. Out-of-profile traffic remains in the queue until it becomes in-profile. When operating in this mode, the queue-scheduling algorithm is considered non-work-conserving, i.e., queued packets are not transmitted at every opportunity, but only when the packets match the Token Bucket profile.

Another mechanism for regulating traffic is metering (as described in the section *Metering*, page *359)* coupled with dropping (as described in the section *Dropping*, page *362*).

The difference between the two mechanisms is that metering/dropping can only mark and optionally drop or forward non-conforming traffic, while shaping can smooth the traffic (by *delaying* non-conforming packets, an operation which metering cannot do).

A token bucket shaper is available per port and a token bucket shaper is available per queue. The port shaper has a higher hierarchical level, meaning that traffic is first shaped by its queue shaper and then shaped for all eight queues of the port by the port shaper.

The Token Bucket shaper is enabled per queue and per port.

## Maximum Transmission Unit (MTU) for Port Shaper

### General

If jumbo MTUs (longer than 2048 bytes) are to be forwarded in shaping mode then, in addition to performing the setting for such MTUs as described in the section *Maximum Transmission Unit (MTU),* page *115*, the setting as described in the section *Custom* (just below) must also be performed. In both settings the MTUs must be at least as large as the jumbo MTUs to be forwarded.

### Custom

To set the Maximum Transmission Unit (MTU) for the port shaper:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **port shaper mtu (1536|2048|10240)**

   where,

   **1536**: MTU size 1536 bytes

   **2048**: MTU size 2048 bytes (default value)

   **10240**: MTU size 10240 bytes.

### Default

To set the MTU for the port shaper to the default value (2048 bytes):

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no port shaper mtu**

## Configuration

For the bandwidth limitation to be met according to the configured traffic shaping as described below, the sizes of the egress packets must not be greater than the MTU size – see the section *Maximum Transmission Unit (MTU) for Port Shaper*, page *376*.

To configure *egress* traffic shaping & bandwidth limitation for one or more queues at one or more ports, invoke the command:

**port egress-shaping [per-queue <1-8>] rate RATELIMIT burst-size BURSTSIZE PORTS-GROUP|all**

where,

**port**: action on port(s).

**egress-shaping**: Shaping of *egress* traffic.

**per-queue**: (optional) Specific queue. If this argument is skipped, the rate limitation will be applied on the port level.

**<1-8>**: Eight queues from which one is to be selected. Queue 1 has CoS/service level 1 (lowest priority). Queue 8 has CoS/service level 8 (highest priority).

**rate**: Rate (bandwidth) limitation.

**RATELIMIT**: Rate limitation. This can be any value in the range **<65k-1g bits/sec>**. The format is a number indexed with **k**, **m**, or **g**
where, **k** = kilo = $10^3$, **m** = mega = $10^6$, **g** = giga = $10^9$. For example, **200m** , which means 200 Mbps. The number is rounded down to a multiple of 65k bits/sec.

**burst-size**: Burst size.

**BURSTSIZE**: Burst size. This can be any value in the range **<4k-16m bytes>**. The format is a number indexed with **k** or **m**
where, **k** = $2^{10}$, **m** = $2^{20}$. For example, **11k** , which means 11K bytes. The number is rounded down to a multiple of 4K bytes.

**PORTS-GROUP**: Group of ports at which the queue(s) is(are) to be rate limited. (Trunk ports may be included in the group. For a trunk, the rate applies to each member port of the trunk and is not the total rate of the entire trunk.)

**all**: All ports at which the queue(s) is(are) to be rate limited.

*Ingress* traffic shaping & bandwidth limitation applies only for a dual port. A dual port has one internal and one external port. For details, refer to the section *Regular, Dual, and Extra Internal Ports*, page *155*. If an analyzer VLAN has been configured on OS912-AC-2 or OS912-DC-2, *internal* Port 10 will become unavailable for *ingress* traffic shaping & bandwidth limitation.

To configure *ingress* traffic shaping & bandwidth limitation for one or more queues at one or more *dual* ports, invoke the command:

**`port ingress-shaping [per-queue <1-8>] rate RATELIMIT burst-size BURSTSIZE PORTS-GROUP|all`**

where,

**`port`**: action on port(s).

**`ingress-shaping`**: Shaping of *ingress* traffic.

**`per-queue`**: (optional) Specific queue. If this argument is skipped, the rate limitation will be applied on the port level.

**`<1-8>`**: Eight queues from which one is to be selected. Queue 1 has CoS/service level 1 (lowest priority). Queue 8 has CoS/service level 8 (highest priority).

**`rate`**: Rate (bandwidth) limitation.

**`RATELIMIT`**: Rate limitation. This can be any value in the range **`<65k-1g bits/sec>`**. The format is a number indexed with **`k`**, **`m`**, or **`g`**
where, **`k`** = kilo = $10^3$, **`m`** = mega = $10^6$, **`g`** = giga = $10^9$. For example, **200m** , which means 200 Mbps. The number is rounded down to a multiple of 65k bits/sec.

**`burst-size`**: Burst size.

**`BURSTSIZE`**: Burst size. This can be any value in the range **`<4k-16m bytes>`**. The format is a number indexed with **`k`** or **`m`**
where, **`k`** = $2^{10}$, **`m`** = $2^{20}$. For example, **11k** , which means 11K bytes. The number is rounded down to a multiple of 4K bytes.

**`PORTS-GROUP`**: Group of dual ports at which the queue(s) is(are) to be rate limited. (Trunk ports may be included in the group. For a trunk, the rate applies to each member port of the trunk and is not the total rate of the entire trunk.)

**`all`**: All ports at which the queue(s) is(are) to be rate limited.

### Example

Below is an example showing the user inputs (in **`bold`**) and OS900 outputs on the CLI screen.

```
MRV OptiSwitch 910 version 1_0_11
OS900 login: admin
Password:
OS900> enable
OS900# configure terminal
OS900(config)# port egress-shaping per-queue 7 rate 200m burst-size 18k 2-4
Note that machine limitation is rate in steps of 65k bits/sec
Note that machine limitation is burst in steps of 4k bytes
port 2 queue 7 egress shaping set to: 199.584m bits/sec 16k bytes
port 3 queue 7 egress shaping set to: 199.584m bits/sec 16k bytes
port 4 queue 7 egress shaping set to: 199.584m bits/sec 16k bytes
OS900(config)#
```

# Memory Resource Management

### General

The OS900 has 4K packet buffers and 4K descriptors. The size of *each* buffer is 256 bytes. These buffers (and descriptors) can be allocated and categorized on the basis of port, queue (SL), and drop-precedence (CL). The remainder of these buffers is automatically allocated as a shared resource/pool (common memory space) for buffering packets (and their descriptors) that may not be immediately stored at their port/queue due to the limited buffer space allocated to the port/queue. This shared resource/pool enables packets with low SL to be forwarded even when their SL buffer budget is exceeded.

| | |
|---|---|
| | **Note** |
| | In allocating buffers, the following requirements must be met:<br>The total of *packet* buffers allocated to all the ports *plus* the buffers allocated as the shared resource does not exceed *4K* and the total of *descriptors* allocated to all the ports *plus* the shared resource does not exceed *4K*. The shared resource is automatically configured to have what is left of the total 4K. Out of the total budget there are some buffers/descriptors allocated for internal use of the device and the automatic configuration of the shared resource takes this allocation into account. |

## Viewing Buffer Usage

To view the buffers used by each queue of each port, enter **`enable`** mode, and invoke the command:

**`show buffers under-use [PORTS-GROUP]`**

where,

**`[PORTS-GROUP]`**: The ports for which buffer usage is to be viewed

<u>Example</u>

```
OS904-DSL4# show buffers under-use 1
Buffers and Descriptors Under Use
=================================
Port: 1
sl<1> Buffers under use:       0   Descriptors under use:       0
sl<2> Buffers under use:       0   Descriptors under use:       0
sl<3> Buffers under use:      27   Descriptors under use:       26
sl<4> Buffers under use:       0   Descriptors under use:       0
sl<5> Buffers under use:      18   Descriptors under use:       15
sl<6> Buffers under use:       0   Descriptors under use:       0
sl<7> Buffers under use:       0   Descriptors under use:       0
sl<8> Buffers under use:       0   Descriptors under use:       0
Port Ingress: 1
sl<1> Buffers under use:       0   Descriptors under use:       0
sl<2> Buffers under use:       0   Descriptors under use:       0
sl<3> Buffers under use:      29   Descriptors under use:      14
sl<4> Buffers under use:       0   Descriptors under use:       0
sl<5> Buffers under use:      22   Descriptors under use:      13
sl<6> Buffers under use:       0   Descriptors under use:       0
sl<7> Buffers under use:       0   Descriptors under use:       0
sl<8> Buffers under use:       0   Descriptors under use:       0
OS904-DSL4#
```

## Buffer Optimization

### Level Setting

To set the level to which the buffers are to be optimized, enter **`configure terminal`** mode, and invoke the command:

**`performance-level (level-1|level-2|level-3|level-4|level-5)`**

where,

**`level-1`**: Regular optimization level (default)

**`level-2`**: Increased optimization level

**`level-3`**: High optimization level

**`level-4`**: Very high optimization level

**`level-5`**: Highest optimization level

<u>Example</u>

```
OS910(config)# performance-level level-3
OS910(config)#
```

**Default Level Setting**

By default, the level to which the buffers are optimized is **`level-1`**.

To set buffer optimization to this level, enter **`configure terminal`** mode, and invoke the command:

**`no performance-level`**

Example

```
OS910(config)# no performance-level
OS910(config)#
```

## Viewing a Buffer Profile

A buffer profile is a global profile defining the buffer resource management for a port. Each port is assigned to one of the 7 global profiles. The buffer profile is only a template defining the buffer limits, but the actual budget is managed per port (not per profile).

To view a global buffer profile, enter **`enable`** mode, and invoke the command:

**`show buffers [profile <1-7>]`**

where,

**`profile`**: Buffer profile.

**`<1-7>`**: Profile number.

Example

```
OS900(config)# show buffers profile 1
Buffer Configuration
====================

Profile 1:
-----------
Port Members: 1-4
Port Ingress Members:
sl<1> Green Buffers:         28   Green Descriptors:         28
sl<1> Red Buffers:            5     Red Descriptors:          5
sl<2> Green Buffers:         28   Green Descriptors:         28
sl<2> Red Buffers:            5     Red Descriptors:          5
sl<3> Green Buffers:         28   Green Descriptors:         28
sl<3> Red Buffers:            5     Red Descriptors:          5
sl<4> Green Buffers:         28   Green Descriptors:         28
sl<4> Red Buffers:            5     Red Descriptors:          5
sl<5> Green Buffers:         28   Green Descriptors:         28
sl<5> Red Buffers:            5     Red Descriptors:          5
sl<6> Green Buffers:         28   Green Descriptors:         28
sl<6> Red Buffers:            5     Red Descriptors:          5
sl<7> Green Buffers:         12   Green Descriptors:         12
sl<7> Red Buffers:            5     Red Descriptors:          5
sl<8> Green Buffers:         12   Green Descriptors:         12
sl<8> Red Buffers:            5     Red Descriptors:          5

Shared Buffers:             648     Descriptors:            434
OS900(config)#
```

The default profile for all ports is Profile 1 as shown in the example above. *Each* port is allocated 120 port buffers, 120 port descriptors. These descriptors and buffers are divided among the two CLs (green, red) and eight SLs (1 to 8) for a port. The shared resource is configured to have 96 shared buffers and 96 shared descriptors.

## Changing a Buffer Profile

Profiles 1 to 6 are user-configurable. Profile 7 is machine-defined and fixed! To change an existing buffer profile, invoke the command:

**`buffers profile <1-6> sl <1-8> <1-4095> <1-4095> <1-4095> <1-4095>`**

where,

**profile**: Buffer profile.

**<1-6>**: Profile number.

**sl**: SL.

**<1-8>**: SL value.

**<1-4095>**: (First appearance) Number of descriptors for green.

**<1-4095>**: (Second appearance) Number of buffers for green.

**<1-4095>**: (Third appearance) Number of descriptors for red.

**<1-4095>**: (Fourth appearance) Number of buffers for red.

Example

```
OS900# configure terminal
OS900(config)# buffers profile 2 sl 5 18 40 3 16
OS900(config)#
```

## Assigning a Buffer Profile to a Port

### Ingress Traffic

To bind any one of 7 global buffer profiles to a port for *ingress* traffic, invoke the command:

**port buffers profile <1-7> ingress [PORTS-GROUP]**

where,

**profile**: Buffer profile.

**<1-7>**: Profile number. Profile 7 is machine-defined, fixed, and allocates much fewer buffers than the *default configuration* of the other profiles.

**ingress**: Ingress traffic.

**[PORTS-GROUP]**: Group of Ports. Default = all ports

Example

```
OS900(config)# port buffers profile 6 ingress 2-4
port 2 buffers profile set to: 6
port 3 buffers profile set to: 6
port 4 buffers profile set to: 6
OS900(config)#
```

### Egress Traffic

To bind any one of 7 global buffer profiles to a port for *egress* traffic, invoke the command:

**port buffers profile <1-7> [PORTS-GROUP]**

where,

**profile**: Buffer profile.

**<1-7>**: Profile number. Profile 7 is machine-defined, fixed, and allocates much fewer buffers than the *default configuration* of the other profiles.

**[PORTS-GROUP]**: Group of Ports. Default = all ports

Example

```
OS900(config)# port buffers profile 2 1,3
port 1 buffers profile set to: 2
port 3 buffers profile set to: 2
OS900(config)#
```

## Restoring the Default Buffer Profile

To restore the default buffer profile for a specific SL, invoke the command:

**no buffers profile <1-6> sl <1-8>**

where,

**profile**: Buffer profile.

**<1-6>**: Profile number.

**sl**: Service Level.

**<1-8>**: Service Level.

Example

```
OS900# configure terminal
OS900(config)# no buffers profile 2 sl 5
OS900(config)#
```

### Allocation of Shared Descriptors and Buffers

The number of buffers and descriptors allocated as the shared resource is automatically configured by the OS900 to the number of buffers and descriptors left after port assignments and internal assignments. To view the shared resource configuration, use the **show buffers [profile <1-7>]** command as described in the section *Viewing a Buffer Profile*, page *379*.

**WARNING!**

It is strongly recommended to use the *default* configuration of buffers and descriptors for memory resource management.

In changing descriptor or buffer budgets, take into account unexpected packet loss.

### Disabling Buffer Sharing

To disable buffer sharing, invoke the command:

```
no buffers shared
```

## Egress Counters

An egress counter is used to count packets in an egress queue according to one or more of the following attributes:

- Physical ports
- VLAN tag (Interface ID)
- Service Level
- Conformance Level

There are two sets of four egress counters, identified as ‘set1’ and ‘set2’. The egress counters in a set are:

- UNICAST (counts the number of unicast packets)
- MCAST/UNKNOWN (counts the number of multicast/unknown packets)
- BCAST (counts the number of broadcast packets)
- TxQ Congest (counts the number of packets dropped due to Tx queue congestion)

### Activation

To activate a set of egress queue counters:

1. Enter **configure terminal** mode.

   Example

   ```
   OS900# configure terminal
   OS900(config)#
   ```

2. Invoke the command:

   ```
   egress-counters (set1|set2) port (PORT|all|skip) tag (<1-4096>|all) sl (<1-8>|all) cl (green|red|all)
   ```

   Or

   ```
   egress-counters (set1|set2) ingress-port (PORT|all|skip) tag (<1-4096>|all) sl (<1-8>|all) cl (green|red|all)
   ```

   where,

   **set1**: First egress counters set

**set2**: Second egress counters set
**port**: Egress port
**ingress-port**: Ingress port
**PORT**: Range of port numbers from which one can be selected
**all**: (first) All ports
**skip**: Skip to the next port after each timeout (1 minute).
**tag**: VLAN interface tag
**<1-4096>**: Range of VLAN Interface IDs from which one can be selected
**all**: (second) All VLAN Interface IDs
**sl**: Egress traffic service level
**<1-8>**: Range of service levels from which one can be selected
**all**: (third) All service levels
**cl**: Egress traffic conformance level
**all**: (fourth) All conformance levels
**green**: Conformance level green
**red**: Conformance level red

To revoke the above command, invoke the command:

**no egress-counters set1|set2**

where,

**set1**: First egress counters set
**set2**: Second egress counters set

Example

```
OS900(config)# egress-counters set1 port 3 tag 2006 sl 5 cl red
OS900(config)#
```

## Viewing

To view the egress queue counters

1. Enter **enable** mode.
2. Invoke either of the following commands:

**show egress-counters set1|set2**
**monitor egress-counters set1|set2**

where,

**show**: Display *without* refresh.
**monitor**: Display *with* refresh.
**set1**: First egress counters set
**set2**: Second egress counters set

Example

```
OS904# show egress-counters set1

EGRESS COUNTERS
===============

Set1: port 3, tag 20, sl 5, cl green
PORT  UNICAST/UNKNOWN MCAST      BCAST      TxQ Congest   STATE
3     0               0          0          0             ENABLE
OS904#
```

# Chapter 21: IEEE 802.1ag and ITU-T Y.1731 Ethernet Service OAM

## General

This chapter presents the OAM functions and mechanisms for Ethernet-based networks, describes the principle of operation of the OS900 with these functions, shows how to configure the OS900 to use these functions and their parameters, gives the procedure for loopback testing, and shows how to view status and performance information.

## Definition

Ethernet Service OAM is a set of management functions for managing Ethernet services. Such management functions are specified in the IEEE 802.1ag and ITU-T SG 13 Y.1731 standards. Ethernet Service OAM includes Fault Management as well as Performance Management (per Y.1731).

## Purpose

The purpose of Ethernet Service OAM is to enable service providers to operate, administer, and maintain Ethernet services. In particular, the path through bridges and LANs taken by frames addressed to and from specified network users can be discovered and verified and faults can be detected and isolated to an individual bridge or LAN.

## Applicability

Ethernet Service OAM can be applied to single-domain and multi-domain Ethernet services.

## Terminology

Following is a list of terms with their meaning as used in this chapter:

**CCM** A multicast CFM PDU transmitted periodically by a MEP in order to verify connectivity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM.

**CFM** An end-to-end[50] per-service-instance-per-VLAN Ethernet layer OAM protocol for proactive connectivity monitoring, fault verification, and fault isolation. These actions are performed using IEEE 802.1ag standard Layer 2 PING, Layer 2 traceroute, and end-to-end connectivity check of Ethernet networks.

**LBR** A unicast CFM PDU transmitted by a MEP or MIP to a MEP, in response to an LBM received from that MEP.

**LTM** A CFM PDU initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating an LTR (**L**ink **T**race **R**eply), up to the point at which the LTM (**L**ink**T**race **M**essage) reaches its destination or can no longer be forwarded.

**MA** A set of MEPs, each configured with the same MAID (**MA ID**entifier) and MD Level (**M**aintenance **D**omain **L**evel), established to verify the integrity of a single service instance. An MA can also be thought of as a full mesh of Maintenance Entities among a set of MEPs so configured.

**MAID** An MA identifier for an MA, unique over the domain that CFM is to protect against the accidental concatenation of service instances. MAID has two parts: the Maintenance Domain Name and the Short MA Name.

---

[50] End-to-end means spanning the Provider Edge or Customer Edge.

| | |
|---|---|
| **MD Level** | **M**aintenance **D**omain Level is a value in the range 0-7 which together with the VLAN tag is used to determine which OAM PDU is to be handled at the current level and which OAM PDU is to be forwarded in the VLAN.<br>OAM allows transparent forwarding of OAM PDUs from higher level domains via lower level domains when the domains are nested.<br>It is possible to set a name for a domain level. This name can be one of following types: DNS, string, or MAC address with a 2-octet unsigned integer. A domain name has to be the same, in respect to type and value, for all MEPs in service. |
| **MDN** | **M**aintenance **D**omain **N**ame is the identifier, unique over the domain for which CFM is to protect against accidental concatenation of service instances, of a particular Maintenance Domain. |
| **ME** | **M**aintenance **E**ntity is a point-to-point relationship between two MEPs within a single MA. |
| **MEG** | **M**aintenance **E**ntity **G**roup is a group of Maintenance Entities. |
| **MEP** | An actively managed OAM entity associated with a specific access port of a service instance that can generate and receive OAM PDUs as well as track any response. It is an end point of a single service that can branch out to other MEPs. This means that a single service may have several MEPs as end points. A MEP resides in a bridge that receives OAM PDUs and transmits them in the direction of the Bridge's Relay Entity. Each MEP maintains a list of MEPs with whom it is connected. Each MEP has a primary VLAN whose tag it sends with OAM PDUs. |
| **MHF** | A CFM entity, associated with a single Maintenance Domain, and thus with a single MD Level and a set of VIDs, that can generate CFM PDUs, but only in response to received CFM PDUs. |
| **MIP** | A CFM entity consisting of one or more MHFs. |
| **Primary VLAN** | The VLAN in a group associated with a service instance, on which all CFM PDUs generated by MPs, except for forwarded LTMs, are to be transmitted. |
| **Service** | A set of MEPs, each configured with the same service ID and MD level, established to verify the integrity of a single service instance. Every service maintains a list of VLANs for whose connectivity it is responsible. The service is uniquely identified by MD level and service name (ID). If the service name is not defined explicitly, it is assigned the first VLAN tag in the list of VLANs. Each service maintains a remote list of MEPs. No OAM request is handled if it arrives from a remote MEP that does not appear on this list. |

# Management Functions

In a layered network model, Ethernet Service OAM is active at the Ethernet Service Layer.

In OAM, a switch (such as the OS900) plays the role of a bridge defining all its Maintenance Entity Groups (MEGs) as MEPs. Each MEP can be uniquely identified by administrative domain level, service ID, and MEP ID. The bridge transmits OAM frames to all ports that belong to the same VLAN except to the MEP ports. A MEP port is required to provide transparency only to higher MD levels.

## Fault Management

The Fault Management OAM contains the following functions, each of which is supported in software:

### Ethernet Continuity Check Function

The Ethernet Continuity Check function (ETH-CC) is used for proactive OAM, i.e., carried out continuously to permit proactive reporting of faults. It causes MEPs to exchange CCMs (**C**ontinuity **C**heck **O**AM Messages) in order to detect Loss Of Continuity (LOC) or incorrect network connections between any pair of MEPs in a MEG.

When ETH-CC is enabled, a MEP periodically transmits CCM PDUs as often as determined by the configured transmission period. When ETH-CC transmission is enabled in a MEG, all MEPs are enabled to periodically transmit frames with ETH-CC information to all other MEPs in the MEG. The ETH-CC transmission period is the same for all MEPs in the MEG. When a MEP is enabled to generate PDUs with ETH-CC information, it also expects to receive PDUs with ETH-CC information from its peer MEPs in the MEG. A MEP always reports reception of a PDU with unexpected ETH-CC information.

A field of flags is incorporated in each CCM. This field is used to indicate the defect detected (if any) and the period during which CCMs are transmitted. In case of a Continuity Fault, a Fault Alarm is generated. Fault Alarm is an out-of-band signal that is both an SNMP notification and a CLI message.

The following defects can be detected by ETH-CC:

**RDI** Remote Defect Indication. It is used by a MEP to communicate to its peer MEPs that a defect condition has been encountered. A MEP that is in a defect condition transmits frames with ETH-RDI information. A MEP, upon receiving frames with ETH-RDI information, determines that its peer MEP has encountered a defect condition.

**MAC** MAC status defect. It is indicated if the:

- o Bridge port on which the transmitting MEP resides, has no ability to pass ordinary data, or
- o MEP's primary VLAN is down.

**RMEP** Remote MEP defect. If no CCM frames are received from a peer MEP within an interval equal to 3.5 times the receiving MEP's CCM transmission period, LOC with the peer MEP is flagged.

**ERROR** Transmission period error. A MEP received a CCM frame with an incorrect value of the transmission period.

**XCON** Cross-connect defect. Incompatibility in one or more of expected parameters in a CCM frame such as: domain level, domain name type, service name type, service ID, etc.

### Ethernet Loopback Function

The Ethernet Loopback Function (ETH-LB) is an on-demand PING-like request/reply OAM function. It causes MEPs to send unicast CFM PDUs called LBMs (**L**oopBack **O**AM **M**essages) to verify connectivity with another MEP for a specific MA. The MEP receiving the LBM responds with an LBR (**L**oopback **R**eply **M**essage). LBRs are used to verify bidirectional connectivity. They are typically initiated by operator command.

Whenever a valid unicast LBM frame is received by a MEP, an LBR frame is generated and transmitted to the requester MEP. A unicast LBM frame with a valid MEG Level and a destination MAC address equal to the MAC address of the receiving MEP is considered to be a valid unicast LBM frame. Every field in the unicast LBM frame is copied to the LBR frame with the following exceptions:

- The source and destination MAC addresses are swapped
- The OpCode field is changed from LBM to LBR

Loopback can also be used as an out-of-service diagnostic test, by transmitting unicast loopback PDUs. The loopback OAM PDU includes a Test Pattern TLV parameter. MRV loopback additionally provides Fame Loss Ratio (FLR) and Frame Delay (FD).

### Ethernet Linktrace Function

The  function causes a MEP to send Link Trace (LT) request PDUs to remote bridges participating in a service on an on-demand basis. Depending on the replies, LT produces a sequence of the bridges from the MEP to the target bridge. The MEP expects to receive LT reply PDUs within a specified period of time. Bridges that do not reply are excluded from the sequence.
LT can be used for:

- Retrieval of adjacency relationships between a MEP and remote bridges participating in the service, i.e., retrieval of the sequence of bridges from the source MEP to the target bridge.
- Fault localization. When a fault (e.g., link or device failure) or a forwarding plane loop occurs, the sequence of bridges will likely be

different from the expected one. The difference in the sequences provides information about the fault location.

## Performance Management

Ethernet Performance Management (ETH-PM) is an on-demand OAM function which causes MEPs to send *PM (*Performance Management) unicast packets to point-to-point MAs. Whenever a valid unicast PM frame is received by the target MEP, a PMR frame is generated and transmitted to the requester MEP. Every field in the PM frame is copied to the PMR frame with the following exceptions:

- The source and destination MAC addresses are swapped.
- The OpCode field is changed from PMM to PMR.
- Rx and Tx time stamps are inserted.

The following performance parameters are measured by respective Performance Measurement[51] messages:

1. Frame Loss Ratio (FLR) – Percentage of undelivered service frames, divided by the total number of service frames during a time interval. The number of service frames not delivered is the difference between the number of service frames sent to an ingress UNI and the number of service frames received at an egress UNI.
2. Frame Delay (FD) - Time taken by a frame to make the round-trip from the source node, through the destination node, and back to the same source node. This time is measured from the start of transmission of the first bit of the frame by a source node until the reception of the last bit of the frame by the same source node.
3. Frame Delay Variation (FDV) or jitter - Measure of the variations in the FD between a pair of service frames belonging to the same CoS instance on a point-to-point Ethernet connection.
4. Inter-arrival jitter – Estimate of the statistical variance of the Performance Measurement data packet inter-arrival time, measured in timestamp units and expressed as an unsigned integer, as defined in RFC1889.

# Configuration

## Rules

The following rules apply when configuring the OS900 to operate Ethernet Service OAM:

1. A user-created service must be assigned a service ID in the range 1 to 65535.
2. Only one MEP may be defined per port.
3. A user-created MEP must be assigned a MEP ID in the range 1 to 4095.
4. MEP is uniquely defined by domain level, service ID, and MEP ID.
5. Port number and VLAN tag uniquely define one MEP.
6. Every port that belongs to the same VLAN of a MEP should *preferably* be tagged.
7. Every MEP that belongs to the same service must be defined in the same *domain level*.
8. Every MEP that belongs to the same service must be defined with the same *domain name*.
9. Every MEP that belongs to the same service must be defined with the same *service ID*.
10. Every MEP that belongs to the same service must be defined with the same *service name*.
11. Every remote MEP that belongs to the same service must be included in the remote MEPs list of the MEP.
12. All remote MEP VLAN tags that belong to the same service must be included in the remote VLANs list of each MEP.
13. The same CCM interval must be defined for all MEPs in the same service.
14. In the same domain, different services must be assigned different primary VLANs.

---

[51] Supported by OS900s with FPGA version `0x19` or later. To view the FPGA version of an OS900, enter **`enable`** mode and invoke the command **`show fpga version`**.

## Network

The network shown in *Figure 40*, below, is used as an example in the procedure for configuring the OS900 to operate Ethernet Service OAM.

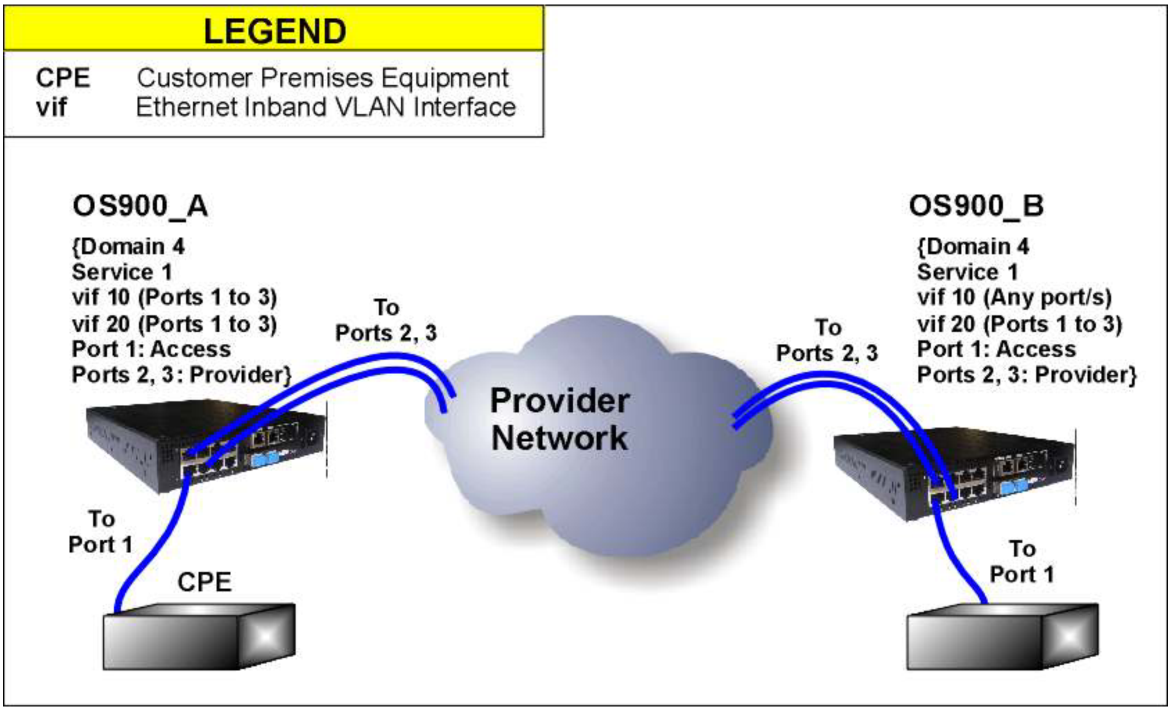



**Figure 40: Network used for Ethernet Service OAM Configuration Procedure**

The planned initial setup is as follows:

- Two bridges (**OS900_A** and **OS900_B**).
- Ethernet VLAN interfaces **vif10** and **vif20** in **OS900_A** and **OS900_B** and participate in service **1** in domain level **4**.
- Ports **1** to **3** are members of inband VLAN interfaces **vif10** and **vif20** in **OS900_A**.
- Port **1** in **OS900_A** is an *access* port.
- Inband VLAN interface **vif10** in **OS900_B** can have any group of ports as members. Although **vif10** here *does not actively* participate in the service, its existence is required because it belongs to the service.
- Ports **1** to **3** are members of inband VLAN interface **vif20** in **OS900_B**.
- Port **1** in **vif20** in **OS900_B** is an *access* port.

## Procedure

Following is the basic procedure for configuring the OS900 to operate Ethernet Service OAM using the network described above as an example. Additional settings may be made using the commands detailed in the section *Optional Configuration Parameters*, page *392*.

**Configuring OS900_A**

1. Set at least one provider port (e.g., **2** or **3** in **OS900_A**) in tagged mode using the command:

   **`port tag-outbound-mode tagged PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Group of ports

   Example

```
OS900_A(config)# port tag-outbound-mode tagged 2,3
OS900_A(config)#
```

2. Create interface VLANs (e.g., `vif10` and `vif20` in **OS900_A**) each including at least two ports (e.g., `1` to `3`)

3. Create an Ethernet OAM domain level (e.g. **4**) using the command:

   **`ethernet oam domain <0-7>`**

   where,

   **`<0-7>`**: Range of eight domain levels from which an integer value is to be selected

   Example

```
OS900_A(config)# ethernet oam domain 4
OS900_A(config-ethoam-Lev4)#
```

   (To *delete* an Ethernet OAM domain level, invoke the command:

   **`no ethernet oam domain <0-7>`**)

4. Create a service (e.g., `1`) in the OAM domain using the command:

   **`service NUMBER (1-65535) or (0x0001-0xffff)`**

   where,

   **`NUMBER`**: Range of service numbers. Either a decimal number from the range **`1-65535`** or a hexadecimal number from the range **`0x0001-0xffff`** may be selected.

   Example

```
OS900_A(config-ethoam-Lev4)# service 1
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

5. To create a MEP on a port, invoke either of the two *equivalent* commands:

   **`mep <1-4095> inward port PORT`**

   **`mep <1-4095> port PORT`**

   where,

   **`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

   **`inward`**: Towards the access port.

   **`PORT`**: Number of port. (The port can be a trunk. Trunks are described in ***Chapter 13:*** *IEEE 802.3ad Link Aggregation (LACP)*, page *273*.)

   (To remove a MEP from a port, invoke the command:

   **`no mep <1-4095> port`**)

6. Select IDs of remote MEPs (e.g., `200` and `300`) that are to participate in the service using the command:

   **`remote-meps LIST-OF-MEPS|all`**

   where,

   **`LIST-OF-MEPS`**: IDs of *remote MEPs*. IDs are to be selected from the range `1` to `4095`

   **`all`**: IDs `1` to `4095`

   Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# remote-meps 200,300
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

   (To *prevent* one or more remote MEPs from participating in the service, invoke the command:

   **`no remote-meps LIST-OF-MEPS|all`**

7. Select VLANs (e.g., `10` and `20`) that are to participate in the service using the command:

   **`vlans LIST-OF-VIDS|all`**

   where,

**LIST-OF-VIDS**: IDs (tags) of *VLANs*. IDs are to be selected from the range **1** to **4095**

**all**: IDs **1** to **4095**

Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# vlans 10,20
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

8. Create a MEP (e.g., **100**) on the access port (e.g., **1**) and assign a VLAN as the primary VLAN (e.g., **10**).

**mep <1-4095> primary-vlan TAG**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**primary-vlan**: Primary VLAN

**TAG**: Primary VLAN ID

Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# mep 100 port 1
OS900_A(config-ethoam-Lev4:MAiD#1)# mep 100 primary-vlan 10
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

(To *delete* a MEP assigned to a primary VLAN, invoke the command:
**no mep <1-4095> primary-vlan**)

(To *delete* a MEP, invoke the command:
**no mep <1-4095>**)

9. Activate the MEP created in step *8* above so that when Ethernet OAM is enabled (as described in step *10* below), MEP can send OAM PDUs.

**mep <1-4095> activate**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**activate**: Activate MEP

Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# mep 100 activate
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

(To *deactivate* a MEP, invoke the command:
**no mep <1-4095> activate**)

10. Enable Ethernet OAM, i.e., create all the entities and enter relative MACs in the learn table by entering **configure terminal** mode and invoking the command:

**ethernet oam enable**

Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# quit
OS900_A(config-ethoam-Lev4)# quit
OS900_A(config)# ethernet oam enable
OS900_A(config)#
```

(To *disable* Ethernet OAM, invoke the command:
**no ethernet oam enable**)

## Configuring OS900 B

Repeat steps *1* to *10*, above, for **OS900_B**.

Example

```
OS900_B(config)# interface vlan vif10
OS900_B(config-vif10)# tag 10
OS900_B(config-vif10)# ports 2-3
OS900_B(config-vif10)# exit
OS900_B(config)# interface vlan vif20
OS900_B(config-vif20)# tag 20
OS900_B(config-vif20)# ports 1-3
OS900_B(config-vif20)# exit
OS900_B(config)# ethernet oam domain 4
OS900_B(config-ethoam-Lev4)# service 1
OS900_B(config-ethoam-Lev4:MAiD#1)# vlans 10,20
OS900_B(config-ethoam-Lev4:MAiD#1)# ccm-interval 10s
OS900_B(config-ethoam-Lev4:MAiD#1)# remote-meps 100,300
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 port 1
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 primary-vlan 20
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 activate

                                  Optional Steps

OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 ccm-activate
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure rmep 100
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure priority 5
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure history-size 10
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure burst-interval 10
OS900_B(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure enable

                                   Continuation

OS900_B(config-ethoam-Lev4:MAiD#1)# exit
OS900_B(config-ethoam-Lev4)# exit
OS900_B(config)# ethernet oam enable
OS900_B(config)#
```

# Optional Configuration Parameters

## Global OAM Parameters

### *Ethernet Header*

To set the OS900 to encapsulate frames with an Ethernet header, invoke the command:

**`ethernet oam encapsulation-type default|llc|type-length`**

where,

**`default`**: Default header, i.e., IEEE 802.3 Standard type header (Type/Length)

**`llc`**: IEEE 802.3 Standard type header followed by IEEE 802.2 LLC Standard type header

**`type-length`**: IEEE 802.3 Standard type header

Example

```
OS900(config)# ethernet oam encapsulation-type type-length
OS900(config)#
```

### *Ethertype*

The OAM ether-type is not specified in the IEEE 802.1ag standard (still to be finalized).

To specify (identify) the OAM ethertype of a frame, invoke the command:

**`ethernet oam ether-type HEXLINE`**

where,

**`HEXLINE`**: Range of OAM ethertypes. Either a *decimal* number from the range `0` to `65535` or a *hexadecimal* number from the range `0x0000` to `0xffff` may be selected. Default: `0x88e6`.

Example

```
OS900(config)# ethernet oam ether-type 0x1a1a
OS900(config)#
```

(To delete specification (identification) of the OAM ethertype of a frame, invoke the command:
**no ethernet oam ether-type [HEXLINE]**)

### *Multicast MAC Address*

The OAM multicast MAC address is not specified in the IEEE 802.1ag standard.

To change a multicast MAC address, invoke the command:
**ethernet oam mac [HEXLINE]**

where,

**HEXLINE**: Range of OAM multicast addresses having the format:
**01:80:c2:** $x_1x_2:x_3x_4:x_5L$, where $x_1x_2:x_3x_4:x_5L$ represent the 6 least significant hex digits of the MAC address, and **L** represents the domain level.
$x_1$ to $x_5$ are to be defined in the future.
Default for **x1x2:x3x4:x5**: **01:80:c2:12:34:5**.

Example

```
OS900(config)# ethernet oam mac 0xaaaaa
OS900(config)#
```

In the example above, **0x** designates hex and **aaaaa** are the values of $x_1$ to $x_5$.

(To revoke changing of a multicast MAC address, invoke the command:
**no ethernet oam mac [HEXLINE]**)

### Destination MAC Address in CCM

To set the multicast destination MAC address in CCMs to be sent by MEPs, invoke the command:
**ethernet oam destination-multicast mac MAC_ADDRESS**

where,

**MAC_ADDRESS**: Multicast destination MAC address in CCMs sent by MEPs in the format **xx:xx:xx:xx:xx:xx** where, **xx** is a double-digit hex number. The first five hex digits are defined in the standard. The value of the last digit as entered by the user is immaterial since it is adjusted by the OS900 automatically.

Example

```
OS900(config)# ethernet oam destination-multicast mac 22:11:55:a3:be:74
dst_mac=22:11:55:a3:be:74
dst_mac=22:11:55:a3:be:70
OS900(config)#
```

To revoke the setting of the multicast destination MAC address in CCMs to be sent by MEPs, invoke the command:
**no ethernet oam destination-multicast mac [MAC_ADDRESS]**

### *TLVs*

A TLV is a datagram consisting of Type, Length, and Value fields. The fields are as follows:

| | |
|---|---|
| **T**ype | Numeric code indicating the kind of field that the message designates |
| **L**ength | Size of the Value field |
| **V**alue | Variable size that contains data for the message |

Setting

To set TLVs (for appending to CCMs), invoke one or both of the following commands:
**ethernet oam organization-specific-tlv set OUI <0-255> length <0-1350>**

or

**ethernet oam organization-specific-tlv set OUI <0-255> VALUE**

where,

**set**: Set

**OUI**: Organizationally Unique Identifier. 6-digit hex number in the format **0xyyyyyy**, where **0x** designates hex. Example: **0x0a0b0c**.

**<0-255>**: Range of type values from which one value is to be selected

**length**: Length of TLV data

**<0-1350>**: Value of TLV data length

**VALUE**: Value of TLV data

| | **Note** |
|---|---|
| | If the Value of length specified is greater than the TLV data length, the data is replicated until it is equal to the length. If the TLV data length is greater than the length specified, the LSB of the data is truncated so that it becomes equal to the length specified. |

Example

```
OS900(config)# ethernet oam organization-specific-tlv set 0xaabbcc 40 length 20
 (Set  organization specific TLV where OUI is 0xaabbcc and sub type is equal to
 40 and length 20.)
```

(To revoke setting of TLVs (for appending to CCMs), invoke the command:

**no ethernet oam organization-specific-tlv set OUI <0-255>**)

Appending

In order to append a specific TLV to CCMs, invoke the command:

**ethernet oam organization-specific-tlv enable OUI <0-255>**

where,

**enable**: Enable

**OUI**: Organizationally Unique Identifier. 6-digit hex number in the format **0xyyyyyy**, where **0x** designates hex. Example: **0x0a0b0c**.

**<0-255>**: Range of type values from which one value is to be selected

Example

```
OS900(config)# ethernet oam organization-specific-tlv enable 0xaabbcc 40
OS900(config)#
```

(To revoke appending of a specific TLV to CCMs, invoke the command:

**no ethernet oam organization-specific-tlv enable**

### Domain Parameters

#### *Encapsulation*

To set the OS900 to encapsulate frames belonging to a given domain level with a specific type, invoke the command:

**encapsulation-type (default|llc|type-length)**

where,

**default**: Default (Type/Length header encapsulation type)

**llc**: LLC header encapsulation type

**type-length**: Type/Length header encapsulation type.

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# encapsulation-type llc
OS900(config-ethoam-Lev4)#
```

#### *Domain Name*

The domain name type and value must be the same for every MEP in a domain.

To assign a domain name type (IEEE 802.1ag compatible), invoke any one of the following commands:

DNS Type

**`name dns NAME`**

where,

**`NAME`**: Name of the domain.

String Type

**`name string NAME`**

where,

**`NAME`**: String (e.g., mnemonic) for the domain.

MAC Address Type

**`name mac-addr-and-uint NUMBER`**

where,

**`NUMBER`**: MAC address with a 2-octet unsigned integer. Decimal number (in the range 0 to 65535) or hex number (in the range 0x0000 to 0xffff).

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# name string MRV-domain
OS900(config-ethoam-Lev4)#
```

### Service Parameters

#### *Enabling a MEP to Send CCM PDUs*

Enable a specific MEP to send CCM PDUs (when Ethernet OAM is enabled).

**`mep <1-4095> ccm-activate`**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

**`ccm-activate`**: Enable sending of CCM PDUs

Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# mep 100 ccm-activate
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

#### *Disabling a MEP from Sending CCM PDUs*

To *disable* a MEP from sending CCM PDUs, invoke the command:

**`no mep <1-4095> ccm-activate`**

#### *CCM Alarms*

By any MEP

*Enabling*

To enable any MEP to send CCM alarms (when Ethernet OAM is enabled) to the *CLI display and Syslog*, enter **`configure terminal`** mode and invoke the command:

**`ethernet oam trace-ccm-fault`**

Example

```
OS912(config)# ethernet oam trace-ccm-fault
OS912(config)#
```

*Disabling*

To disable all MEPs from sending CCM alarms to the *CLI display and Syslog*, enter **`configure terminal`** mode and invoke the command:

**`no ethernet oam trace-ccm-fault`**

Example

```
OS912(config)# no ethernet oam trace-ccm-fault
OS912(config)#
```

By a Specific MEP

*Enabling*

To enable a specific MEP to send CCM alarms (when Ethernet OAM is enabled) to *an SNMP manager*, enter the **service** mode of the MEP and invoke the command:

**mep <1-4095> ccm-alarms (all|fault|recovery)**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**ccm-alarms**: Enable sending of CCM alarms

**all**: Send *nbEthOamCcmAlarm* PDU when MEP loses or restores contact with one or more remote MEPs

**fault**: Send *nbEthOamCcmAlarm* PDU when MEP loses contact with one or more remote MEPs

**recovery**: Send *nbEthOamCcmAlarm* PDU when MEP restores contact with one or more remote MEPs (default)

Example

```
OS912(config-ethoam-Lev4:MAiD#1)# mep 100 ccm-alarms
OS912(config-ethoam-Lev4:MAiD#1)#
```

To enable a specific MEP to send CCM alarms (when Ethernet OAM is enabled) to the *CLI display and Syslog*, enter the **service** mode of the MEP and invoke the command:

**mep <1-4095> trace-ccm-faults**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS912(config-ethoam-Lev4:MAiD#1)# mep 223 trace-ccm-faults
OS912(config-ethoam-Lev4:MAiD#1)#
```

*Disabling*

To *disable* a specific MEP from sending CCM alarms to an SNMP manager, enter the **service** mode of the MEP and invoke the command:

**no mep <1-4095> ccm-alarms (all|fault|recovery)**

where,

**all**: Send *nbEthOamCcmAlarm* PDU when MEP loses or restores contact with one or more remote MEPs

**fault**: Send *nbEthOamCcmAlarm* PDU when MEP loses contact with one or more remote MEPs

**recovery**: Send *nbEthOamCcmAlarm* PDU when MEP restores contact with one or more remote MEPs (default)

Example

```
OS912(config-ethoam-Lev4:MAiD#1)# no mep 100 ccm-alarms fault
OS912(config-ethoam-Lev4:MAiD#1)#
```

To *disable* a specific MEP from sending CCM alarms to the *CLI display and Syslog*, enter the **service** mode of the MEP and invoke the command:

**no mep <1-4095> trace-ccm-faults**

Example

```
OS912(config-ethoam-Lev4:MAiD#1)# no mep 223 trace-ccm-faults
OS912(config-ethoam-Lev4:MAiD#1)#
```

***Time between CCM PDUs***

To set the time interval between CCM PDUs, invoke the command:

**ccm-interval TIME_INTERVAL**

where,

**TIME_INTERVAL**: Time interval between CCM PDUs.
Choices: **100ms**, **10ms**, **10s**, **1s**, **300Hz** ($3^{1}/_{3}$ millisecond), **600s**, and **60s**. Default: **1s** (1 second).

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# ccm-interval 10s
OS900(config-ethoam-Lev4:MAiD#1)#
```

(To reset the time interval between CCM PDUs to the default value, invoke the command:
**no ccm-interval**)

| | |
|---|---|
| | **Note**<br>The chosen time interval between CCM PDUs must be the same in every MEP in a service. |

**InterfaceStatusTLV in CCM**

By default, MEPs send the InterfaceStatusTLV with the CCM.

To cause a MEP to send the InterfaceStatusTLV, invoke the command:

**mep <1-4095> send-interface-tlv**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config-ethoam-Lev4:MAiD#1)# mep 44 send-interface-tlv
OS900(config-ethoam-Lev4:MAiD#1)#
```

To prevent a MEP from sending the InterfaceStatusTLV, invoke the command:

**no mep <1-4095> send-interface-tlv**

***PortStatusTLV in CCM***

By default, MEPs send the PortStatusTLV with the CCM.

To cause a MEP to send the PortStatusTLV, invoke the command:

**mep <1-4095> send-port-tlv**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS910(config-ethoam-Lev4:MAiD#1)# mep 44 send-port-tlv
OS910(config-ethoam-Lev4:MAiD#1)#
```

To prevent a MEP from sending the PortStatusTLV, invoke the command:

**no mep <1-4095> send-port-tlv**

***Lowest CCM Defect Priority***

The order of priority of CCM defects is as follows: MAC (lowest priority) < RDI < Remote_MEP < ERROR < XCON (highest priority). These defects are described in the section *Ethernet Continuity Check Function*, page *386*.

To set the lowest CCM defect priority that will issue an alarm, invoke the command:

**mep <1-4095> lowest-alarm-prio (all|error|mac_status|none|rdi|rmep)**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**lowest-alarm-prio**: CCM with the lowest-priority defect that is allowed to generate a Fault Alarm

**all**: All defects, i.e., XCON CCM, ErrorCCM, Remote MEP fault, RDI, and MACStatus

**error**: ErrorCCM, Remote_MEP fault, RDI, MACStatus

**mac_status**: RDI and MACStatus

**none**: Not alarm (for any of the defects)

**rdi**: RDI

**rmep**: Remote_MEP, RDI, or MACStatus is received.

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 lowest-alarm-prio rmep
OS900(config-ethoam-Lev4:MAiD#1)#
```

To revoke issuing of alarms when a CCM defect is detected, invoke the command:

**no mep <1-4095> lowest-alarm-prio**

### *Layer 2 VLAN Tag Priority CCM or Linktrace*

To set a Layer 2 VLAN tag priority for handling OAM PDUs of the *CCM* or *Linktrace* function that are transmitted from a specific MEP, invoke the command:

**mep <1-4095> priority [<0-7>]**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<0-7>**: Range of priorities. Default: 0.

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 priority 2
OS900(config-ethoam-Lev4:MAiD#1)#
```

To reset the Layer 2 VLAN tag priority for OAM PDUs (that are transmitted from a specific MEP), to the default value, invoke the command:

**no mep <1-4095> priority**

### *CCM Priority Mismatch Alarm*

Enabling

To generate an alarm when a mismatch occurs between the configured priority bits and that in the received CCM packet, and also to preassign a CCM defect priority to such an alarm, invoke the command:

**mep <1-4095> check-priority (error|xcon)**

where,

**error**: Indicate ERROR defect for a mismatch between the priority bits.

**xcon**: Indicate XCON defect for a mismatch between the priority bits.

Example

```
OS900(config-ethoam-Lev4:MAiD#1)# mep 200 check-priority xcon
OS900(config-ethoam-Lev4:MAiD#1)#
```

Disabling

By default, no is generated when a mismatch occurs between the configured priority bits and that in the received CCM packet. To disable generation of such an alarm, invoke the command:

**no mep <1-4095> check-priority [error|xcon]**

### *Service Name Type and Value*

To define the service name type and value, invoke either of the following two commands:

Primary VID Type Name

**name primary-vid <1-4095>**

where,

**primary-vid**: Primary VID type.

**<1-4095>**: Name of the service (primary VID).

> **Note**
> The service name type and value must be the same for every MEP in a specific service.

<u>String Type Name</u>

**`name string NAME`**

where,

**`string`**: String type.

**<NAME>**: Name of the service (e.g., mnemonic).

<u>Example</u>

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# name primary-vid 10
OS900(config-ethoam-Lev4:MAiD#1)#
```

To revoke the service name type and value, invoke the command:

**`no name`**

### *Default Primary-VLAN for MEPs*

To create a default primary-VLAN for every MEP in service, invoke the command:

**`primary-vlan <1-4095>`**

where,

**<1-4095>**: Range of VLANs.

<u>Example</u>

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# primary-vlan 10
OS900(config-ethoam-Lev4:MAiD#1)#
```

To delete the default primary-VLAN, invoke the command:

**`no primary-vlan`**

## Defect and Alarm Parameters

### *Fault Alarm Invocation Wait Time*

To set the time that defects must be *present* before a Fault Alarm is issued, invoke the command:

**`mep <1-4095> fng-alarm-time [TIME_INTERVAL]`**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**`TIME_INTERVAL`**: Time for defects to be present.

Choices: **`100ms`**, **`10ms`**, **`10s`**, **`1s`**, **`2.5s`**, **`300Hz`** ($3^1/_3$ millisecond), **`600s`**, and **`60s`**. Default: **`1s`** (1 second).

<u>Example</u>

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 fng-alarm-time 1s
OS900(config-ethoam-Lev4:MAiD#1)#
```

To reset the time that defects must be *present* before a Fault Alarm is issued, invoke the command:

**`no mep <1-4095> fng-alarm-time`**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

### *Fault Alarm Revocation Wait Time*

To set the time that defects must be *absent* before a Fault Alarm is disabled, invoke the command:

**`mep <1-4095> fng-reset-time [TIME_INTERVAL]`**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

**`TIME_INTERVAL`**: Time for defects to be absent.
Choices: **`100ms`**, **`10ms`**, **`10s`**, **`1s`**, **`2.5s`**, **`300Hz`** ($3^1/_3$ millisecond), **`600s`**, and **`60s`**. Default: **`1s`** (1 second).

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 fng-reset-time 10s
OS900(config-ethoam-Lev4:MAiD#1)#
```

To reset the time that defects must be *absent* before a Fault Alarm is disabled, invoke the command:

**`no mep <1-4095> fng-reset-time`**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

### *Thresholds*

Frame-Delay/Jitter

To set the Performance Monitoring frame-delay or jitter thresholds for averages in a burst that will cause alarms to be sent to the CLI or SNMP manager when crossed, invoke the command:

**`mep <1-4095> threshold (frame-delay|ds-jitter|sd-jitter) rise <0-100000> fall <0-100000>`**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

**`frame-delay`**: Frame delay

**`ds-jitter`**: Destination-Source jitter

**`sd-jitter`**: Source-Destination jitter

**`<0-100000>`**: (First appearance) Rise threshold value (microseconds). It is the maximum time in microseconds *above* which an alarm is sent.

**`<0-100000>`**: (Second appearance) Fall threshold value (microseconds). This value must not exceed the *Rise* threshold value. It is the minimum time in microseconds *below* which an alarm is sent.

Example

```
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 threshold frame-delay rise 200 fall 150
OS900(config-ethoam-Lev4:MAiD#1)#
```

To revoke the Performance Monitoring threshold setting, invoke the command:

**`no mep <1-4095> threshold (frame-delay|ds-jitter|sd-jitter) [rise] [NUMBER] [fall] [NUMBER]`**

Example

```
OS900(config-ethoam-Lev4:MAiD#1)# no mep 100 threshold frame-delay
OS900(config-ethoam-Lev4:MAiD#1)#
```

Packet-Loss

To set the Performance Monitoring packet-loss thresholds for averages in a burst that will cause alarms to be sent to the CLI or SNMP manager when crossed, invoke the command:

**`mep <1-4095> threshold packet-loss rise <0-100> fall <0-100>`**

where,

**packet-loss**: Packet loss

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<0-100>**: (First appearance) *Rise* threshold value. It is the % packet loss *above* which an alarm is sent. This alarm indicates *impermissible* packet loss.

**<0-100>**: (Second appearance) *Fall* threshold value. It is the % packet loss *below* which an alarm is sent. This alarm indicates *permissible* packet loss. The *Fall* threshold value must be *less than* the *Rise* threshold value.

Example

```
OS910(config-ethoam-Lev4:MAiD#1)# mep 100 threshold packet-loss rise 15 fall 14
OS910(config-ethoam-Lev4:MAiD#1)#
```

To revoke the Performance Monitoring threshold setting, invoke the command:

**no mep <1-4095> threshold packet-loss [rise] [NUMBER] [fall] [NUMBER]**

Example

```
OS910(config-ethoam-Lev4:MAiD#1)# no mep 100 threshold packet-loss
OS910(config-ethoam-Lev4:MAiD#1)#
```

### Delay-Measurement/Loss-Measurement/Loopback Parameters

#### *General*

Delay-Measurement, Loss-Measurement, and Loopback tests are run between two OS900s.

In delay measurement testing, the elapsed time is measured for the round-trip path of a packet sent from an OS900.

In loss measurement testing, the number of packets lost is measured in each of the two directions in a round-trip path from an OS900.

In loopback testing, receipt/loss of a packet is verified for its round-trip path from an OS900.

Up to four tests[52] can be run concurrently.

However, over a 100 tests can be preset and run either by the internal mechanism of the OS900 or using the scheduler function described in ***Chapter 27:*** *Scheduler*, page *499*. Using this function, the tests (each time-limited) are preset to be run in succession. As soon as any of four tests is completed, the next test is automatically run.

The internal mechanism schedules running of the tests in round-robin fashion. That is, as soon as a test runs one burst of packets[53] it is sent to the end of the wait queue if it is scheduled to run more than once. (Such scheduling can be done using the command in the section *Number of Bursts*, page *402*). Here the test waits until the end of its burst interval and until it reaches the front of the queue. As soon as one of the four tests running concurrently is completed, the test is run again.

For Delay-Measurement or Loopback, the remote MEP(s) must be specified in the service by invoking either of the commands in the section *Remote MEPs*, page *401*.

#### *Service Level (SL)*

To set the SL for a MEP, invoke the command:

**mep <1-4095> (delay-measure|loopback) sl <1-8>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-8>**: SL to be selected from the range 1 to 8

To reset the SL for a MEP to the default value (`1`), invoke the command:

**no mep <1-4095> (delay-measure|loopback) sl**

#### *Remote MEPs*

To select the remote (destination) MEPs for a MEP, use either of the following methods.

---

[52] The tests can be RFC 2544, IP SLA, Y.7131 Delay Measurement, and Y.7131 Loopback.

[53] The number of packets to be sent in a burst interval can be set using the command given in the section *Number of Packets, page 405*.

Method 1 (Remote MEP identified by its *ID*)

To select the local MEP and remote MEPs (between which the Delay-Measurement, Loss-Measurement, or Loopback testing is to be performed):

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loss-measure|loopback rmep (<1-4095>|LIST-OF_MEPS)**

where,

**<1-4095>**: (First appearance) *Local* MEP ID to be selected from the range 1 to 4095

**<1-4095>**: (Second appearance) Single *Remote* MEP ID to be selected from the range 1 to 4095

**<LIST-OF_MEPS>**: Multiple *remote* MEP IDs to be selected from the range 1 to 4095

(To *revoke* selection of remote MEPs, invoke the command:

**no mep <1-4095> delay-measure|loss-measure|loopback rmep**.)

Method 2 (Remote MEP identified by its *MAC Address*)

To select the local MEP and remote MEPs (between which the Delay-Measurement is to be set or Loopback testing is to be performed)

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback mac MAC_ADDRESS**

where,

**<1-4095>**: *Local* MEP ID to be selected from the range 1 to 4095

**MAC_ADDRESS**: MAC address of the *remote* MEP in hex format, e.g., `aa:bb:cc:dd:ee:ff`

(To *revoke* selection of remote MEPs, invoke the command:

**no mep <1-4095> delay-measure|loopback mac**.)

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure mac 00:0F:BD:00:36:57
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure enableOS900(config-ethoam-Lev4:MAiD#1)#
```

***Number of Bursts***

To set the number of frame transmission bursts:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback burst-number <1-255>|forever**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-255>**: Number of bursts to be selected from the range 1-255. Default: **1**

**forever**: Continuous transmission

To reset the burst number to the default value, invoke the command:

**no mep <1-4095> delay-measure|loopback burst-number**

***Number of History Entries***

To limit the number of most recent history entries:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loss-measure|loopback history-size <2-65535>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<2-65535>**: Maximum number of history entries to be recorded from the range 2 to 65535. Default: **5**

(To reset the number of history entries to the default value, invoke the command:
**no mep <1-4095> delay-measure|loss-measure|loopback history-size**)

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure history-size 20
```

### *Time Interval*

To set the time interval between every two packets in a burst

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback interval <1-1000> [msec| μsec]**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-1000>**: Time interval to be selected from the range 1 to 1000. Default: **100**

**[msec| μsec]**: milliseconds or microseconds. Default: **msec** (milliseconds)

(To reset the time interval to the default value, invoke the command:
**no mep <1-4095> delay-measure|loopback interval**)

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure interval 200
OS900(config-ethoam-Lev4:MAiD#1)#
```

### *Layer 2 VLAN Tag Priority for Delay-Measurement or Loopback*

To set the Layer 2 VLAN tag priority for OAM PDUs of the *Delay-Measurement* or *Loopback* function that are transmitted from a specific MEP

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback priority <0-7>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<0-7>**: VLAN tag priority. Default: Same as MEP priority

(To reset the Layer 2 VLAN tag priority to the default value, invoke the command:
**no mep <1-4095> delay-measure|loopback priority**)

### *Wait Time*

To set the maximum time the Delay-Measurement/Loss-Measurement/Loopback mechanism is to wait for a response to its request PDU:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loss-measure|loopback timeout <0-60000>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<0-60000>**: Wait time (in milliseconds) from the range 0 to 60000. Default: **200**

(To reset the wait time to the default value, invoke the command:
**no mep <1-4095> delay-measure|loss-measure|loopback timeout**

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure timeout 10000
OS900(config-ethoam-Lev4:MAiD#1)#
```

### *CLI Messages*

To cause the display of a CLI message for every Delay-Measurement or Loopback attempt (i.e., reply by echoing the PDU from the local MEP)

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback echo-reply-mode**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**echo-reply-mode**: Reply by echoing the PDU from the local MEP.

(By default CLI messages are not displayed.To prevent display of CLI messages, invoke the command:

**no mep <1-4095> delay-measure|loopback echo-reply-mode**)

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure echo-reply-mode
OS900(config-ethoam-Lev4:MAiD#1)#
```

### *PDU Length*

To set the PDU length (measured in the Layer 2 header up to and excluding CRC) that will help diagnose faults sensitive to this length:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback length <60-9000>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<60-9000>**: PDU length (in octets) to be selected from the range 60 to 9000. If the MEP is enabled for CPU-based measurement (using the command **mep <1-4095> (delay-measure|loopback) enable [slow]** described in the section *Activating*, page *405*), then the PDU length is to be selected from the range 60 to 1496. Default: **60**

(To reset the PDU length to the default value, invoke the command:

**no mep <1-4095> delay-measure|loopback length**)

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure length 80
OS900(config-ethoam-Lev4:MAiD#1)#
```

### *Data Pattern*

To set a data pattern (inside a PDU) that will help to diagnose faults sensitive to incompleteness of data in a frame:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback pattern HEXLINE**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**HEXLINE**: Pattern (dataFill) of DataTLV using hexadecimal digits, e.g., **0f0f0a0a880c**

If a conflict exists between PDU length and pattern size, the whole pattern is used.

(To delete the data pattern, invoke the command:

**no mep <1-4095> delay-measure|loopback pattern**

### *Layer 2 PDU Priority*

To set the Layer 2 PDU priority:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback priority [<0-7>]**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**[<0-7>]**: Layer 2 PDU priority to be selected from the range 0 to 7. Default: Same as MEP priority

(To reset the Layer 2 PDU priority to the default value, invoke the command:
**no mep <1-4095> delay-measure|loopback priority**

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 delay-measure priority 5
OS900(config-ethoam-Lev4:MAiD#1)#
```

***Number of Packets***

To set the number of packets to be sent during each burst interval:

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback packets <1-1000000>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-1000000>**: Number of packets to be sent to be selected from the range 1 to 1000000. Default: **3**.

(To reset the number of packets to be sent to the default value, invoke the command:
**no mep <1-4095> delay-measure|loopback packets**

***Burst Interval***

To set the time interval between every two bursts

For a *specific* MEP in the service, invoke the command:

**mep <1-4095> delay-measure|loopback burst-interval <1-86400>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-86400>**: Burst interval (in seconds) to be selected from the range 1 to 86400. Default **60**.

To reset the burst interval to the default value, invoke the command:
**no mep <1-4095> delay-measure|loopback burst-interval**

***Activating***

To activate the PDU Delay-Measurement, Loss-Measurement, or Loopback function, invoke the command:

**mep <1-4095> (delay-measure|loss-measure|loopback) enable [slow]**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**[slow]**: *CPU-based* Delay-Measurement, Loss-Measurement, or Loopback. (This argument exists only for OS900s having an FPGA.)

Default: *Hardware-accelerated* Delay-Measurement, Loss-Measurement, or Loopback. (*Hardware-accelerated* Delay-Measurement, Loss-Measurement, or Loopback provides for presenting time parameters with extremely higher accuracy, i.e., in nanoseconds!)

For OS900s having an FPGA, *CPU-based* Delay-Measurement, Loss-Measurement, or Loopback is optional. For OS900s that do not have an FPGA, *CPU-based* Delay-Measurement, Loss-Measurement, or Loopback is enforced.

In *hardware-accelerated* Delay-Measurement, Loss-Measurement, or

Loopback, the maximum length allowed for packets is 9000 bytes. In *CPU-based* Delay-Measurement, Loss-Measurement, or Loopback, the maximum length allowed is 1500 bytes.

Alternatively, Delay-Measurement/Loss-Measurement/Loopback can be activated in **enable** mode by invoking the command: **ethernet oam domain <0-7> service NUMBER mep <1-4095> delay-measure|loss-measure|loopback enable**.

Example 1

```
OS900_A(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure enable
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

Example 2

```
OS900_A(config-ethoam-Lev4:MAiD#1)# mep 200 delay-measure enable slow
Results of delay measure for Level=4 MA=1 MEPiD=200:
 Started:Sat Mar  4 17:57:22 2000 on target: rmep 201 mac
00:0f:bd:01:5e:88
 10 packets transmitted; 10 packets received, 0.00% packet loss
Round-trip min/avg/max:    2.526/15.585/44.248 ms
    Jitter SD min/avg/max: 0.000/ 2.278/ 11.212 ms; number=10
    Jitter DS min/avg/max: 0.000/ 8.655/ 41.205 ms; number=10
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

The results of Delay-Measurement/Loopback can be viewed by invoking any of the commands in the section *Viewing History Entries*, page *417*.

***Deactivating***

To deactivate the PDU Delay-Measurement, Loss-Measurement, or Loopback mechanism, invoke the command:

**no mep <1-4095> (delay-measure|loss-measure|loopback) enable**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**Storm Guard**

A storm guard can be enabled over a group of ports, i.e., the ports can be set to automatically disconnect from the network when a user-specified ingress OAM frame rate is exceeded.

Enabling

To enable a storm guard over a group of ports, invoke the command:

**ethernet oam pdu-storm-guard [VALUE] PORTS-GROUP|all**

where,

**VALUE**: Maximum number of OAM PDUs per port per second.

**PORTS-GROUP**: Group of ports

**all**: All ports

Example

```
OS900(config)# ethernet oam pdu-storm-guard 7 3-5
OS900(config)#
```

Disabling

By default, storm guard is disabled. To disable storm guard over a group of ports, invoke the command:

**no ethernet oam pdu-storm-guard PORTS-GROUP|all**

where,

**PORTS-GROUP**: Group of ports

**all**: All ports

Example

```
OS900(config)# no ethernet oam pdu-storm-guard 3-5
OS900(config)#
```

Reconnecting Ports

To reconnect the ports to the network after they have been disconnected by the storm guard, invoke the command:

**port state enable PORTS-GROUP|all**

where,

**enable**: Enable

**PORTS-GROUP**: Group of ports

**all**: All ports

Example

```
OS900(config)# port state enable 2
port 2 state set to: ENABLE
OS900(config)#
```

### Ignoring MEPs

To cause the OS900 to ignore certain or all MEPs, invoke the command:

**ignore-rmeps (all|LIST-OF-MEPS)**

where,

**all**: Ignore all remote MEPs

**LIST-OF-MEPS**: Specify the IDs (from the range **1-4095**) of the remote MEPs to be ignored.

To revoke the ignore command (above), invoke the command **no ignore-rmeps (all|LIST-OF-MEPS)**.

### Aging of Remote MEPs

By default, aging of remote MEPs is disabled.

#### *Enabling*

To enable aging of remote MEPs, invoke the command:

**remote-meps aging <0-86400>**

where,

**<0-86400>**: Aging time (in seconds) of remote MEPs to be selected in the range 0-86400. 0 disables aging.

#### *Disabling*

To disable aging of remote MEPs, invoke the command:

**no remote-meps aging [NUMBER]**

where,

**[NUMBER]**: Existing aging time (in seconds) of remote MEPs.

## Customer Ports

Customer ports can be set to operate in the IEEE 802.1ag and ITU-T SG 13 Y.1731 standards. However, such customer ports will not be able to transmit CCM packets.

### Per Domain

To set customer ports for a whole domain:

1. Enter/create an Ethernet OAM domain level using the command:

   **ethernet oam domain <0-7>**

   where,

   **<0-7>**: Range of eight domain levels from which an integer value is to be selected.
2. Invoke the command:

   **c-ports PORTS-GROUP**

where,

**PORTS-GROUP**: Group of ports to be set as customer ports.

Example

```
OS912C(config-ethoam-Lev4)# c-ports 2-5,8
OS912C(config-ethoam-Lev4)#
```

**Per Service**

To set customer ports for a specific service in a domain:

1. Enter/create an Ethernet OAM domain level using the command:
   **ethernet oam domain <0-7>**
   where,
   **<0-7>**: Range of eight domain levels from which an integer value is to be selected.
2. Enter/create a service in the OAM domain using the command:
   **service NUMBER (1-65535) or (0x0001-0xffff)**
   where,
   **NUMBER**: Range of service numbers. Either a decimal number from the range **1-65535** or a hexadecimal number from the range **0x0001-0xffff** may be selected.
3. To set customer ports for the specific service, invoke the command:
   **c-ports PORTS-GROUP**
   where,
   **PORTS-GROUP**: Group of ports to be set as customer ports.

Example

```
OS900_A(config-ethoam-Lev4:MAiD#1)# c-ports 2-5,8
OS900_A(config-ethoam-Lev4:MAiD#1)#
```

# Viewing

## Ethernet OAM Defaults

To view the default settings for Ethernet OAM parameters:

1. Enter **enable** mode
2. Invoke the command:
   **show ethernet oam defaults**

Example

```
OS906C# show ethernet oam defaults
Parameter                       Default values
----------------------------------------------------------------
OAM:
  destination-multicast          01:80:C2:00:00:3y
  enable                         no
  encapsulation-type             3
  ether-type                     8902
  organization-specific-tlv      no
  pdu-storm-guard                50 OAM PDUs per port per second
Domain:
  encapsulation-type             3
Service:
  ccm-interval                   1 sec
  name                           The same as service index
  primary-vlan                   1
Mep:
  activate                       no
  ccm-activate                   no
  ccm-alarms                     recovery
  fng-alarm-time                 2.5 sec
  fng-reset-time                 10 sec
  lowest-alarm-prio              rdi
  primary-vlan                   The same as service primary-vlan
  send-interface-tlv             yes
  send-port-tlv                  yes
  threshold                      0 usec
Linktrace:
  ttl                            255
  use_fdb_only                   yes
DM/LB:
  burst-interval                 60 sec
  burst-number                   1
  echo-reply-mode                no
  history-size                   5 entries
  interval                       100 msec
  length                         60 bytes (without CRC)
  packets                        3
  priority                       The same as MEP priority
  timeout                        200 msec
OS906C#
```

## Selected Domain Levels

To display the list of selected domain levels, from domain's or service's mode invoke the command:

**show domains**

Example 1 (from *domain* mode)

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# show domains
Level  NameType(##)   Name
    4 None    ( 1) -
End of Table.
OS900(config-ethoam-Lev4)#
```

Example 2 (from *service* mode)

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show domains
Level  NameType(##)   Name
    4 None    ( 1) -
End of Table.
OS900(config-ethoam-Lev4:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `Level` | Number of domain level |
| `NameType` | DNS, character string, MAC address with 2-octet integer, user defined (i.e., a number outside the IEEE 802.1ag standard range), or none |
| `(##)` | Name type code |
| `Name` | Maintenance Domain Name in the format specified for the Maintenance Domain NameType. |

## List of MEPs in a Domain

To display the list of all MEPs in a given domain, from the domain's mode invoke the command:
**`show mep status`**

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# show mep status
Service Lev=4:Ma#1
mepid port act cc-act vid mac
  100    1   Y    Y    10 00:0F:BD:00:36:57
End of Table.
OS900(config-ethoam-Lev4)#
```

The fields in the above example are described below.

| | |
|---|---|
| `mepid` | ID of MEP (in a specific domain and service) |
| `port` | Bridge port on which the MEP resides |
| `act` | `Y`: MEP activated, `N`: MEP idle |
| `cc-act` | `Y` –MEP enabled to send CCM PDUs, `N`: MEP disabled from sending CCM PDUs |
| `vid` | Primary VLAN ID (tag) |
| `mac` | MEP port MAC address |

## Status of All Services

To view the Continuity Check (CC) status of *all services* in a specific domain, in the domain's mode invoke the command:
**`show ccm`**

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# show ccm

Service Lev=4:Ma#1
MEPiD Port VID RDI MAC RMEP ERROR XCON highestDefect rCCMseq.Errors  Tx  Rx
100   2    20  n   Up  n    n     n    XCON          0               843 736

Service Lev=4:Ma#1
MEPiD Port VID RDI MAC RMEP ERROR XCON highestDefect rCCMseq.Errors  Tx  Rx
200   1    10  Y   Dn  n    n     n    MACStatus     0               217 211

End of Table.
OS900(config-ethoam-Lev4)#
```

The fields in the above example are described below.

| | |
|---|---|
| `MEPid` | ID of local MEP (in a specific domain and service) |
| `Port` | Bridge Port on which the MEP resides |
| `VID` | Primary VLAN ID (tag) |
| `RDI` | `Y`: MEP in RDI state<br>`N`: MEP *not* in RDI state |
| `MAC` | `Up`: A CCM with a MAC TLV or interface TLV has been received. `Dn`: No CCM with a MAC TLV or interface TLV has been received. |
| `RMEP` | `Y`: A CCM with a CCM Interval field that contains a non-zero value has been received.<br>`N`: No CCM with a CCM Interval field that contains a non-zero value has been received. |
| `ERROR` | `Y`: An invalid CCM has been received.<br>`N`: No invalid CCM has been received. |
| `XCON` | `Y`: One or more cross-connect CCMs has been received, and 3.5 times of at least one of those CCMs' transmission interval has not yet expired.<br>`N`: One or more cross-connect CCMs has been received and/or 3.5 times of at least one of those CCMs' transmission interval has not yet expired. |
| `Highest Defect` | The highest priority defect that occurred in the MEP. (The order of priority of defects is as follows: MAC [lowest] < RDI < RMEP < ERROR < XCON [highest].) |
| `rCCMseq.Errors` | Number of frames received with a wrong sequence number |
| `Tx` | Number of CCM frames transmitted by MEP |
| `Rx` | Number of CCM frames received by MEP |

## List of MEPs in a Service

To display the list of all MEPs in a specific service, from the service's mode invoke the command:

**`show mep status`**

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep status
mepid port act cc-act vid mac
  100    2   n    n     0 00:00:00:00:00:00
End of Table.
OS900(config-ethoam-Lev4:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `mepid` | ID of MEP (in a specific domain and service) |
| `port` | Bridge port on which the MEP resides |
| `act` | `Y`: MEP activated, `N`: MEP idle |
| `cc-act` | `Y` –MEP enabled to send CCM PDUs, `N`: MEP disabled from sending CCM PDUs |
| `vid` | Primary VLAN ID (tag) |
| `mac` | MEP port MAC address |

## MEP Status

To display the status of a specific MEP, from the service's mode invoke the command:

**`show mep status <1-4095>`**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep status 100
mepid port act cc-act vid mac
  100    2   n    n     0 00:00:00:00:00:00
End of Table.
OS900(config-ethoam-Lev4:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `mepid` | ID of MEP (in a specific domain and service) |
| `port` | Bridge port on which the MEP resides |
| `act` | `Y`: MEP activated, `N`: MEP idle |
| `cc-act` | `Y` –MEP enabled to send CCM PDUs, `N`: MEP disabled from sending CCM PDUs |
| `vid` | Primary VLAN ID (tag) |
| `mac` | MEP port MAC address |

## OAM Configuration

To view the Ethernet OAM configuration, from a domain or service mode invoke the command:

**`show configuration`**

Example (from *service* mode)

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show configuration
!
! Ethernet OAM configuration
!
ethernet oam domain 4
  service 1
    vlans 10,20
    remote-meps 100,200,300
    mep 100 port 2
    mep 100 primary-vlan 10
    mep 100 activate
    mep 100 ccm-activate
ethernet oam enable
OS900(config-ethoam-Lev4:MAiD#1)#
```

## List of Remote MEPS Linked to a Local MEP

To display the list of remote MEPs linked to a specific local MEP in a service, from the service's mode invoke the command:

**`show mep <1-4095> rmeps`**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep 100 rmeps

  Remote MEPs of the MEP MEPiD=100 of Lev=4:Ma#1

  MEPiD  srcPort  State  lastChangeTime  MAC                RDI  Port  IfStat  RxCCMs
  200    2        OK     19:35:05,83     00:0F:BD:00:22:79  Y    Down  Down    20976

End of Table.
OS900(config-ethoam-Lev4:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `mepid` | ID of remote MEP (in a specific domain and service) |
| `srcPort` | Number of port that receives frames from remote MEP |
| `State` | Idle / start / fault / OK |
| `LastChangeTime` | The last time the state of the MEP changed |
| `MAC` | Remote MEP port MAC address |
| `RDI` | `Y`: RDI flag is enabled in CCM frames belonging to a specific remote MEP.<br>`N`: RDI flag is disabled |
| `Port` | `Up`: The Bridge Port on which the remote MEP resides can pass ordinary data regardless of the status of the MAC.<br>`Down`: Bridge Port on which the remote MEP resides cannot pass ordinary data. |
| `IfStat` | `Up`: The status of the interface on which the MEP is transmitting the CCM is configured.<br>`Down`: The status of the interface on which the MEP is transmitting the CCM is not configured. |
| `RxCCMs` | Number of received CCM frames. |

## CC Status of a Specific Service

To view Continuity Check (CC) status of a *specific service*, from the service's mode invoke the command:

**`show ccm`**

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show ccm

Service Lev=4:Ma#1
MEPiD Port  VID RDI MAC RMEP ERROR XCON highestDefect rCCMseq.Errors  Tx  Rx
100   1     10  Y   Dn  n    n     n    MACStatus     0               251 210

End of Table.
OS900(config-ethoam-Lev4:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `mepid` | ID of remote MEP (in a specific domain and service) |
| `Port` | Bridge Port on which the MEP resides |
| `VID` | Primary VLAN ID (tag) |
| `RDI` | `Y`: MEP in RDI state<br>`N`: MEP *not* in RDI state |
| `MAC` | `Up`: A CCM with a MAC TLV or interface TLV has been received. `Dn`: No CCM with a MAC TLV or interface TLV has been received. |
| `RMEP` | `Y`: A CCM with a CCM Interval field that contains a non-zero value has been received.<br>`N`: No CCM with a CCM Interval field that contains a non-zero value has been received. |
| `ERROR` | `Y`: An invalid CCM has been received.<br>`N`: No invalid CCM has been received. |
| `XCON` | `Y`: One or more cross-connect CCMs has been received, and 3.5 times of at least one of those CCMs' transmission interval has not yet expired.<br>`N`: One or more cross-connect CCMs has been received and/or 3.5 times of at least one of those CCMs' transmission interval has not yet expired. |
| `Highest Defect` | The highest priority defect that occurred in the MEP. (The order of priority of defects is as follows: MAC [lowest] < RDI < RMEP < ERROR < XCON [highest].) |

| | |
|---|---|
| `rCCMseq.Errors` | Number of frames received with a wrong sequence number |
| `Tx` | Number of CCM frames transmitted by MEP |
| `Rx` | Number of CCM frames received by MEP |

## Time Interval between CCM PDUs

To view the time interval between CCM PDUs, invoke the command:

**`show ccm interval`**

Example

```
OS900(config-ethoam-Lev4:MAiD#1)# show ccm interval
  1s
OS900(config-ethoam-Lev4:MAiD#1)#
```

## Defects in CCMs in a Specific MEP

To display *all* defects indicated in CCMs for a specific MEP, in the service's mode invoke the command:

**`show mep ccm defects <1-4095>`**

where,

**`defects`**: All defects

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep ccm defects 100

Service Lev=4:Ma#1
MEPiD Port VID RDI MAC RMEP ERROR XCON highestDefect rCCMseq.Errors  Tx   Rx
100   1   10   Y   Dn  n    n     n    MACStatus     0               226  210

End of Table.
OS900(config-ethoam-Lev4:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `mepid` | ID of remote MEP (in a specific domain and service) |
| `Port` | Bridge Port on which the MEP resides |
| `VID` | Primary VLAN ID (tag) |
| `RDI` | `Y`: MEP in RDI state<br>`N`: MEP *not* in RDI state |
| `MAC` | `Up`: A CCM with a MAC TLV or interface TLV has been received. `Dn`: No CCM with a MAC TLV or interface TLV has been received. |
| `RMEP` | `Y`: A CCM with a CCM Interval field that contains a non-zero value has been received.<br>`N`: No CCM with a CCM Interval field that contains a non-zero value has been received. |
| `ERROR` | `Y`: An invalid CCM has been received.<br>`N`: No invalid CCM has been received. |
| `XCON` | `Y`: One or more cross-connect CCMs has been received, and 3.5 times of at least one of those CCMs' transmission interval has not yet expired.<br>`N`: One or more cross-connect CCMs has been received and/or 3.5 times of at least one of those CCMs' transmission interval has not yet expired. |
| `Highest Defect` | The highest priority defect that occurred in the MEP. (The order of priority of defects is as follows: MAC [lowest] < RDI < RMEP < ERROR < XCON [highest].) |
| `rCCMseq.Errors` | Number of frames received with a wrong sequence number |
| `Tx` | Number of CCM frames transmitted by MEP |

`Rx` Number of CCM frames received by MEP

## *Cross-Connect* Defects in CCMs in a Specific MEP

To display *cross-connect* defects (**XCON**) indicated in CCMs for a specific MEP, in the service's mode invoke the command:

**`show mep ccm xcon <1-4095>`**

where,

**`xcon`**: Cross-connect defects

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep ccm xcon 100
```

## *Remote MEP* Defects in CCMs in a Specific MEP

To display defects indicated in CCMs for *remote MEPs*, in the service's mode invoke the command:

**`show mep ccm rmep-error <1-4095>`**

where,

**`rmep-error`**: Remote MEP defects

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep ccm rmep-error 100
```

## CCM Received Last in a Specific MEP

To display the CCM received last in a specific MEP, in the service's mode invoke the command:

**`show mep ccm last-ccm <1-4095>`**

where,

**`last-ccm`**: CCM received last

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show mep ccm last-ccm 100
```

## Delay-Measurement/Loopback/Loss-Measurement Status

To view the latest Delay-Measurement, Loopback, or Loss-Measurement test status for a *specific* MEP or *all* MEPs:

1. Enter the mode of the service for which the Delay-Measurement, Loopback, or Loss-Measurement status(es) of the MEP(s) is (are) to be viewed
2. Invoke the command:

   **`show (delay-measure|loopback|loss-measure) history [mep <1-4095> [rmep LIST-OF-MEPS]]`**

   where,

   **`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

   **`LIST-OF-MEPS`**: Remote MEP IDs to be selected from the range 1 to 4095

The keyword **`history`** in the above command is mandatory for Loss-Measurement.

If the optional parameter **[mep <1-4095>]** is not used, the Delay-Measurement, Loopback, or Loss-Measurement statuses of all the MEPs are displayed.

Example

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# show loopback

Service Lev=4:Ma#1
mepid Active NextId ExpectID Absent rmepid
  100     No      0        0      0      0
 Started:Sun Jan  0 00:00:00 1900 on target: mac b3:90:ce:a7:9b:6d
 200 packets transmitted; 200 packets received, 0.00% packet loss
OS900(config-ethoam-Lev4:MAiD#1)#
```

### CCM Status

To view the CCM configuration for all MEPs:

1. Enter **enable** mode
2. Invoke the command:
   **show ethernet oam ccm**

**show ethernet oam delay-measure|loss-measure|loopback**

**show ethernet oam linktrace [detailed-output]**

**show running-config ethernet [oam]**

## Cross-Connect Alarm Notifications

The Cross-Connect (CC) alarm notification format is as follows:

```
EthOam Fault:XXX MEP={Level=L MA=0xM MEPiD=N} sysUpTime=HH:MM:SS,MS
```

where,

XXX: Defect type MAC Status, RDI, Remote MEP, Error, or Cross-Connect
L: Domain level
M: Service ID
N: MEP ID
sysUpTime: Time elapsed since reboot until detection of the defect type.
HH: hours
MM: minutes
SS: seconds
MS: milliseconds

**Note**
Note that the defect type in a MEP is indicated if it occurred during sysUpTime.

Example

Below is an example of a CC alarm notification.

```
EthOam Fault:MACStatus MEP={Level=4 MA=0x1 MEPiD=100} sysUpTime=00:01:23,75
```

## History

### Setting Number of Loopback History Entries

To set the *number* of latest loopback history entries (bursts) whose results are to be displayed for a specific MEP, invoke the command:

**mep <1-4095> loopback history-size <2-65535>**

where,

**`<1-4095>`**: Local MEP ID to be selected from the range 1 to 4095

**`loopback`**: Loopback

**`history-size`**: History entries to be held

**`<2-65535>`**: Range of numbers of history entries. Default: **`5`**.

## Viewing History Entries

### Whole History

To view the whole history of CLI commands invoked, from **`enable`** mode or a **`service`** mode invoke the command:

**`show history`**

### Delay-Measurement/Loss-Measurement/Loopback History

Results of Delay-Measurement/Loss-Measurement/Loopback History are displayed with *ns* accuracy if *hardware-accelerated* Delay-Measurement/Loss-Measurement/Loopback was enabled using the command **`mep <1-4095> (delay-measure|loss-measure|loopback) enable`** described in the section *Activating*, page *405*.

#### *All MEPs*

To view Delay-Measurement/Loss-Measurement/Loopback history for all MEPs:

From **`enable`** mode invoke the command:

**`show ethernet oam delay-measure|loss-measure|loopback history`**

or

From a **`service`** mode invoke the command:

**`show delay-measure|loss-measure|loopback history`**

Example 1

```
OS906C(config-ethoam-Lev0:MAiD#1)# show delay-measure history

Service Lev=0:Ma#1

------------- id:1 -------------
 Started:Tue Jun 30 16:50:01 2009 fast
on target: rmep 60 mac 00:0f:bd:3c:5e:85 priority: 4
 3 packets transmitted; 3 packets received, 0.00% packet loss
Round-trip min/avg/max:   13.424/13.333/13.520 us
Jitter SD min/avg/max:   -1.104/-1.136/-1.168 us
Jitter DS min/avg/max:     1.104/1.120/1.136 us
OS906C(config-ethoam-Lev0:MAiD#1)#
```

The fields in the above example are described below.

| | |
|---|---|
| `fast` | Hardware-accelerated test mode (measurement with 1 ns accuracy) |
| `slow` | CPU-based test mode (measurement with 1 ms accuracy) |
| `priority` | IEEE 802.1p VPT (in the range 0-7) |
| `Round-trip min` | Minimal value of frame round-trip time (in µs, with 1 ns accuracy) |
| `Round-trip avg` | Average value of frame round-trip time (in µs, with 1 ns accuracy) |
| `Round-trip max` | Maximal value of frame round-trip time (in µs, with 1 ns accuracy) |
| `JitterSD min` | Minimal value of source-destination jitter (in µs, with 1 ns accuracy) |
| `JitterSD avg` | Average value of source-to-destination jitter (in µs, with 1 ns accuracy) |

| | |
|---|---|
| `JitterSD max` | Maximal value of source-to-destination jitter (in µs, with 1 ns accuracy) |
| `JitterDS min` | Minimal value of destination-to-source jitter (in µs, with 1 ns accuracy) |
| `JitterDS avg` | Average value of destination-to-source jitter (in µs, with 1 ns accuracy) |
| `JitterDS max` | Maximal value of destination-to-source jitter (in µs, with 1 ns accuracy) |

Example 2

```
OS906C(config-ethoam-Lev1:MAiD#14)# show loopback history

Service Lev=1:Ma#14

------------- id:11 -------------
 Started:Sat Apr 15 19:31:26 2000 on target: rmep 201 mac
00:0f:bd:01:5e:88
 10 packets transmitted; 10 packets received, 0.00% packet loss
OS906C(config-ethoam-Lev1:MAiD#14)#
```

***Specific MEP***

To view the Delay-Measurement/Loss-Measurement/Loopback history for a specific MEP, from the mode of a **`service`** invoke the command:

**`show delay-measure|loss-measure|loopback history mep <1-4095>`**

Example 1

```
OS900(config-ethoam-Lev4:MAiD#1)# show delay-measure history mep 100
Service Lev=4:Ma#1
OS900(config-ethoam-Lev4:MAiD#1)#
```

Example 2

```
OS900(config-ethoam-Lev4:MAiD#1)# show loopback history mep 100
Service Lev=4:Ma#1
OS900(config-ethoam-Lev4:MAiD#1)#
```

# Link Trace

The Link Trace (LT) function causes a MEP to send LT request PDUs to remote bridges participating in a service on an on-demand basis. Depending on the replies, LT produces a sequence of the bridges from the MEP to the target bridge. The MEP expects to receive LT reply PDUs within a specified period of time. Bridges that do not reply are excluded from the sequence.

LT can be used for:

- Retrieval of adjacency relationships between a MEP and remote bridges participating in the service, i.e., retrieval of the sequence of bridges from the source MEP to the target bridge.
- Fault localization. When a fault (e.g., link or device failure) or a forwarding plane loop occurs, the sequence of bridges will likely be different from the expected one. The difference in the sequences provides information about the fault location.

## Setting

### Activation

To activate the link trace function, invoke the command:

**`mep <1-4095> linktrace rmep <1-4095>`**

or

**`mep <1-4095> linktrace mac MAC_ADDRESS`**

where,

**`<1-4095>`**: (First appearance) Local (source) MEP ID to be selected from the range 1 to 4095

**<1-4095>**: (Second appearance) Remote (destination) MEP ID to be selected from the range 1 to 4095

**MAC_ADDRESS**: MAC address of the remote MEP

Additional parameter to these commands is the number of link trace packets that should be transmitted in one burst.

Example 1

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 linktrace rmep 200

MEP={Level=4 MA=1 MEPiD=100}  from 00:0F:BD:01:22:79 id=1 ttl=254 Terminated

OS900(config-ethoam-Lev4:MAiD#1)#
```

Example 2

```
OS900(config)# ethernet oam domain 4
OS900(config-ethoam-Lev4)# service 1
OS900(config-ethoam-Lev4:MAiD#1)# mep 100 linktrace mac 00:0F:BD:01:22:79
```

The fields in the above example are described below.

| | |
|---|---|
| `MEP={Level=4 MA=1 MEPiD=100}` | Domain Level 4, Service 1, and MEP ID 100 |
| `LTR(port 2)` | Link Trace Reply arrived at Port 2 |
| `00:0F:BD:01:22:79` | Responder MAC address |
| `Id=1` | LT message sequence number |
| `ttl=254` | Time to leave (starts from 255) |
| `Terminated` | Receipt of reply from target (destination) MAC address |

**Packet Handling Mode**

To set the linktrace packet handling mode, invoke the command:

**mep <1-4095> linktrace (clear|use_fdb_only)**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**clear**: Use only FDB for LTM forwarding

**use_fdb_only**: (UseFDBonly from 802.1ag-2007): It indicates that only MAC addresses learned in a Bridge's Filtering Database, and not information saved in the MIP CCM Database, is to be used to determine the Egress Port.

(To reset the linktrace packet handling mode to the default (**clear**), invoke the command:

**no mep <1-4095> linktrace use_fdb_only**)

**Time-To-Live**

To set the time-to-live for linktrace packets, invoke the command:

**mep <1-4095> linktrace ttl <1-255>**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-255>**: Time-to-live for linktrace packets from the range 1 to 255. Default: **255**

To reset the time-to-live to the default value (255), invoke the command:

**no mep <1-4095> linktrace ttl**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

## Viewing

To view the linktrace setting for a MEP, invoke the command:

**show linktrace [mep <1-4095>] [detailed-output]**

where,

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

# Automatic Scheduling of Delay Measurement, Loopback, and Link Trace

To schedule an individual Delay-Measurement, Loopback, or Link Trace operation, invoke a scheduler command, as described in ***Chapter 27:*** *Scheduler.*, page *499*.

Example

```
OS910> enable
OS910# configure terminal
OS910(config)# schedule extended 7
OS910(sched-7)# start-time now
OS910(sched-7)# end-time Feb 6 14:25
OS910(sched-7)# interval 1
OS910(sched-7)# command cli ethernet oam domain 4 service 1 mep 2 delay-measure
enable
OS910(sched-7)# enable
```

In the above example:

The *first* **enable** enables the delay-measurement function

The *second* **enable** enables the scheduler.

# Clearing MEP Statistics

To clear all statistics on a MEP:

1. Enter the mode of the specific service (by invoking the command **service NUMBER**) whose MEP statistics are to be cleared.
2. Invoke the command:

   **mep <1-4095> clear-all-statistics**

   where,

   **<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

# Debug

## Type of CCM Message to Send

To select the type of message a specific MEP is to send:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **debug ethernet oam domain <0-7> service NUMBER interfaces|(mep <1-4095> port <1-223> activation|ccm-freeze|dmm|fng|rx-ccm|tx-ccm)**

   where,

   **activation** Port activation

   **ccm-freeze** CCM Freezing

   **dmm** Delay Measurement/Loopback tests start/stop

   **fng** Fault Notification Generator

   **rx-ccm** CCM PDU Reception

   **tx-ccm** CCM PDU Transmission

To revoke the type of message a specific MEP is to send, invoke the command:

**no debug ethernet oam domain <0-7> service NUMBER interfaces|(mep <1-4095> port <1-223> activation|ccm-freeze|dmm|fng|rx-ccm|tx-ccm)**

## CCM Message Destination

To select the destination to which messages of a specific MEP are to be sent:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`debug ethernet oam target (all|cli|console|current-session|log)`**

   where,

   | | |
   |---|---|
   | **`all`** | All targets |
   | **`cli`** | CLI (Telnet/Ssh) sessions |
   | **`console`** | System console |
   | **`current-session`** | Current CLI session |
   | **`log`** | System log |

   To revoke the destination to which messages of a specific MEP are to be sent, invoke the command:

To revoke the destination to which messages of a specific MEP are to be sent, invoke the command:

**`no debug ethernet oam target (all|cli|console|current-session|log)`**

# Chapter 22 IEEE 802.3ah OAM for Ethernet in the First Mile

## Terminology

The terms and their meanings as used in this chapter are as follows:

| Term | Meaning |
|---|---|
| **OAM**(**O**perations **A**dministration, and **M**aintenance) | Tools/utilities for installing, monitoring, and troubleshooting a network. |
| **CO** | Central Office (Local) OAM device.<br>Examples are: OptiSwitch 900, OptiSwitch 940, OptiSwitch 9124-410G, and OptiSwitch 9000. |
| **BO** | Branch Office (Remote or CPE) OAM device.<br>Examples are: OS-300, OptiSwitch 900, OptiSwitch 940, OptiSwitch 9124-410G, OptiSwitch 9000, EM316GRMAHSH, and EM316EFRMAHSH. |
| **OESD** | EM316GRMAHSH or EM316EFRMAHSH. |
| **EFM** (**E**thernet in the **F**irst **M**ile) | Technology used to implement the OAM protocol over the link connecting a CO port (e.g., MRV OS9000 port) to a BO port (e.g., MRV OS900 port). |
| **OUI** (**O**rganization **U**nique **I**dentifier) | Vendor-specific information. |
| **PDU** (**P**rotocol **D**ata **U**nit) | OAM PDU. |
| **TLV** (**T**ype-**L**ength-**V**alue) | Data consisting of Type, Length, and Value fields. These fields are as follows:<br>**T**ype Numeric code indicating the kind of field that the message designates<br>**L**ength Size of the Value field<br>**V**alue Variable size that contains data for the message |
| **loc-port** (local port) | In a CLI command, a CO port. |
| **rm-port** (remote port) | In a CLI command, a BO port. |
| **mrv** | In a CLI command, OESD. |

## General

Implementation of OAM for EFM in the OptiSwitch is based on the IEEE 802.3ah standard. This standard specifies OAM protocols and Ethernet interfaces for management over Ethernet in the First Mile (EFM). The OAM sublayer is within the Data Link Layer of the OSI model. The OAM protocol defines mechanisms to monitor the health of a network link and locate faults using the *transport* layer [IEEE 802.3ah clause 57]. These mechanisms include the following set of functions:

– EFM link performance monitoring
– Fault detection
– Loopback testing
– Setting of network event types to be announced

Vendor specific extensions are allowed to provide functions such as station management, bandwidth allocation, and provisioning.

The OAM sublayer software:

- Supports a single instance of the OAM entity and OAM client [ah 57.2-57.6];
- Operates in passive mode [ah 57.2.9];
- Facilitates the notification of critical events [ah 57.2.10];
- Provides a data link layer frame-level loopback mode [ah 57.2.11]; and
- Utilizes basic (untagged) IEEE 802.3 frames or OAM Protocol Data Units (OAMPDUs), to convey standard and vendor-specific information [ah 57.4].

The number of OAM frames is usually limited to as little as ten per second, so there should be no appreciable impact on the user traffic stream under normal conditions.

The OAM frames are fixed-size and can be distinguished from other frames by the Destination MAC address and the Ethernet type & subtype.

# Purposes

The IEEE 802.3ah OAM protocol has two purposes:

- To enable management of a customer network device without the need for the IP protocol.
- To provide reliable service assurance mechanisms for provider as well as customer networks so as to avoid expensive time-consuming in-the-field truck rolls for isolating faults.

# Application

A common application for the OAM functions is to Ethernet-in-the-First-Mile (EFM) networks. Each such network, as shown in *Figure 41*, below, consists of:

- A port of a CO
- The cable connecting a port of a CO to a port of a BO
- The port of a BO

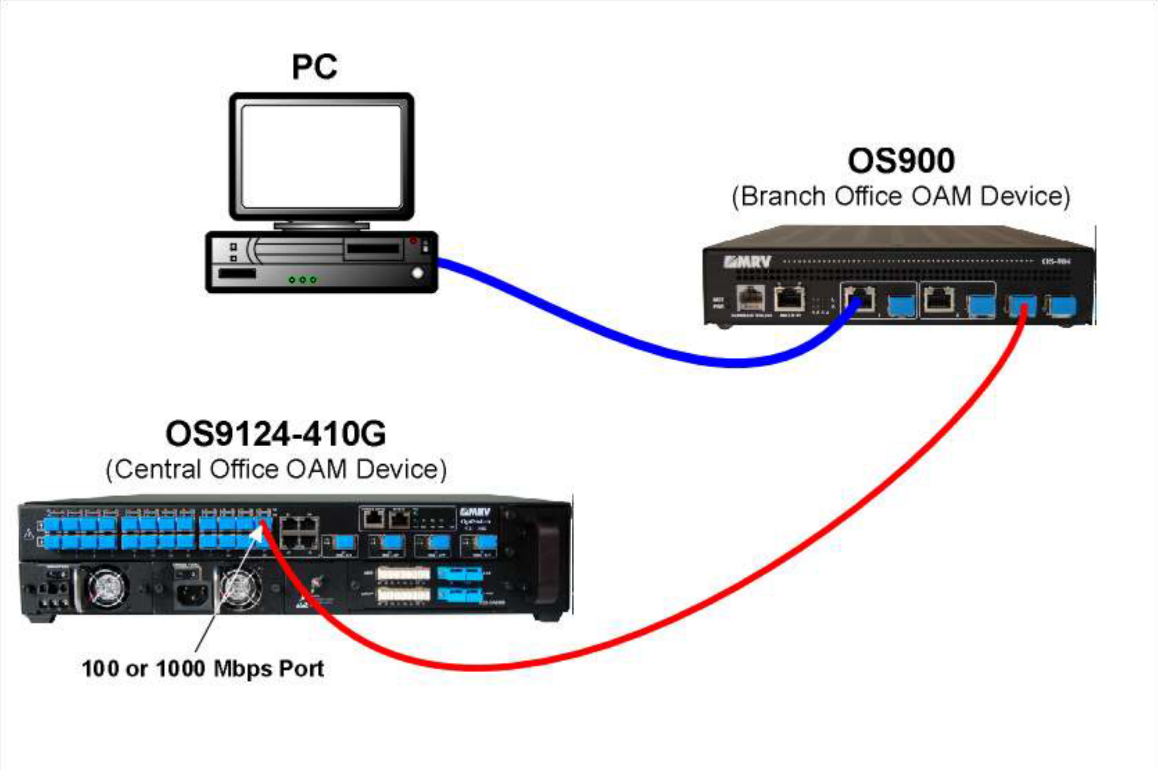



**Figure 41: EFM Link for Running the IEEE 802.3ah OAM Protocol**

# Advantages

EFM networks implemented with MRV's OptiSwitches provide the following advantages:

- Single-point of management
- Low-cost simple IP-less solution (i.e., the devices do not need IP provisioning or IP addresses)
- Branch Office power failure indication
- End-to-end built-in self test for the fiberoptic link
- Independent of traffic loads, network configuration changes, and IP connectivity failure

# Branch Office OAM Device

## Requirement

The BO must meet the OAM protocol requirements specified in the IEEE 802.3ah standard.

## Capability

To view the capabilities of the BO:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show efm-cpe cfg-capability`**

Example

```
OS900# show efm-cpe cfg-capability
Name                             Default     Current
Field                            (Supported)
-----------------------------   ----------  ----------
Variable Request              : Yes         Yes
Link Events Notification      : No          No
Loopback                      : Yes         Yes
Unidirectional                : No          No
OS900#
```

## Operational Mode

As a passive OAM sublayer, the OptiSwitch begins transmitting Information OAMPDUs only after receiving one. The exchange of Information OAMPDUs and agreement on parameters advances the discovery process to the SEND_ANY state, allowing any OAMPDU to be sent.

The OAM sublayer uses a timer to limit transmission of OAMPDUs (ten per second), and to ensure that at least one is sent every second. A second timer detects loss of expected traffic.

## Critical Events

Critical events are signaled using flag bits that are present in every OAMPDU sent.

## Dying Gasp

### General

Indicates time to failure due to power outage.

The dying gasp indication (trap) is always sent to the CO.

A power recovery indication is also sent when power is returned to the OptiSwitch.

If a Layer 3 connection is present between the OptiSwitch and an SNMP host (manager) the dying gasp trap is sent directly to the SNMP host.

The procedure for configuring hosts that are to receive dying gasps (and other traps) is described in the section *Trap Host Specification*, page *338*.

**Supporter Models**

*Table 16*, below, shows which models of the OS900 have the dying gasp transmission capability.

**Table 16: Dying Gasp Capability for Models**

| Model | Dying Gasp Capability |
|---|---|
| OS904 | Yes |
| OS906 | Yes |
| OS910 | No |
| OS910-M | No |
| OS912 | Yes |
| OS930 | No |
| OS940 | Yes |
| OS9124-410G | No |

**Traps**

***Number Setting***

To set the number of OAMPDUs each incorporating a dying gasp critical link event that are to be sent from the BO to the CO:

1. Enter **`configure terminal`** mode. (This can be done from **`configure terminal`** mode.)
2. Invoke the command:

   **`efm-cpe dying-gasp-trap <1-30>`**

   where,

   **`<1-30>`**: Number of OAMPDUs each incorporating a dying gasp critical link event.

Example

```
OS900(config)# efm-cpe dying-gasp-trap 4
OS900(config)#
```

***Number Viewing***

To view the number of OAMPDUs each incorporating a dying gasp critical link event that are set for sending from the BO to the CO:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`show efm-cpe dying-gasp-trap`**

Example

```
OS900# show efm-cpe dying-gasp-trap
Number of dying-gasp alarms (traps) to be send is 4
OS900#
```

## Loopback

Loopback is performed on the OptiSwitch port that is connected to the CO.

The CO may instruct the BO to enter loopback mode. In this mode, the BO end OAM sublayer will return all packets received and the initiating OAM sublayer will discard them. Packet and byte count statistics will be kept to assist in diagnosing link problems.

The OptiSwitch PHY interfaces can be tested in a loopback mode. Performing a loopback on a port via a BO management interface may cause loss of connectivity to that management port.

### Activation

Before activating the IEEE 802.3ah Ethernet OAM protocol, make sure that the ports of the BO to participate in this protocol are ***not*** set to tagged mode. For setting of modes, refer to the section *Outbound Tag Mode*, page *137*.

To activate the IEEE 802.3ah Ethernet OAM protocol, invoke the command:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **efm-cpe ports PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports to operate with IEEE 802.3ah OAM.

Example

```
OS900(config)# efm-cpe ports 2-4
OS900(config)#
```

To deactivate the IEEE 802.3ah Ethernet OAM protocol, invoke the command:

**no efm-cpe ports PORTS-GROUP**

where,

**PORTS-GROUP**: Group of ports to operate with IEEE 802.3ah OAM.

## Central Office OAM Device

### General

The EFM CLI commands are used to monitor, configure, and collect statistical information on EFM links.

These commands are presented under the sections *Setting OAM Configuration*, page *427*, and *Viewing OAM Status*, page *434*. Each of these sections is partitioned into two subsections: ‘COs’ and ‘BOs.’

All EFM commands are invoked at the **efm** mode of the OS900. To enter the **efm** mode, execute the following sequence of commands after login:

**enable → configure terminal → efm**

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# efm
OS900(config-efm)#
```

### Requirement

The CO must meet the OAM protocol requirements specified in the IEEE 802.3ah standard.

### Setting OAM Configuration

#### CO

##### *Enabling OAM Protocol*

To enable the IEEE 802.3ah OAM protocol on the OS900, invoke the command:

**enable**

Example

```
OS900(config-efm)# enable
OS900(config-efm)#
```

> **Note**
>
> Enabling the IEEE 802.3ah OAM protocol on the OS900 does *not* enable the OS900 ports to participate in the IEEE 802.3ah OAM protocol. To enable OS900 ports, the OS900 must be enabled as described above in this section and the ports must be enabled as described in the section *Enabling Ports*, page *428*.

### *Disabling OAM Protocol*

By default, the IEEE 802.3ah OAM protocol is disabled on the OS900.

To disable the IEEE 802.3ah OAM protocol in any case, invoke the command:

**no enable**

Example

```
OS900(config-efm)# no enable
OS900(config-efm)#
```

### *Enabling Ports*

To enable specific OS900 ports to participate in OAM:

1. Ensure that the ports to be enabled to participate in OAM are set to a *non-tag* mode. (For setting a port to a non-tag mode, refer to ***Chapter 6:*** *Ports*, section *Outbound Tag Mode*, page *137*.)
2. Invoke the command:

   **ports PORTS-GROUP|all**

   where,

   **PORTS-GROUP** Group of ports to participate in OAM.

   **all** All ports to participate in OAM.

Example

```
OS900(config-efm)# ports 3-7
OS900(config-efm)#
```

### *Disabling Ports*

An OS900 port must first be disabled from participating in OAM in order to perform the following actions:

- Setting the port in tag mode.
- Adding/deleting the port to/from an OS900 interface.
- Deleting an OS900 interface having the port as a member.

By default, the OS900 ports are disabled from participating in the IEEE 802.3ah OAM protocol.

To disable specific OS900 ports from participating in OAM, invoke the command:

**no ports PORTS-GROUP|all**

where,

**PORTS-GROUP** Group of ports to be disabled ports from participating in OAM.

**all** All ports to be disabled ports from participating in OAM.

Example

```
OS900(config-efm)# no ports 3-7
OS900(config-efm)#
```

### *Enabling/Disabling Loopback on a BO*

To enable/disable loopback on a *BO*, invoke the command:

**rm config loc-port PORT loopback off|on**

where,

**PORT** OS900 port that is connected to the BO.

**off** Disable loopback on the BO.

**on** Enable loopback on the BO.

Example

```
OS900(config-efm)# rm config loc-port 7 loopback on
OS900(config-efm)#
```

| | **Note** |
|---|---|
| | To view the loopback status of a *BO* that is connected to an OS900 port:<br>1) Invoke the command:<br>**`show oam-config loc-port PORT target-device remote`**<br>as described in the section *Viewing OAM Status of an OESD*, page *437*.<br>2) In the display, read the line beginning with '`Loopback Ctrl`' |

***Enabling Discarding of Packets Looped Back via BO***

By default, packets that are looped back via the BO are discarded.

To enable packets that are looped back via the BO to be discarded, invoke the command:

**`discard-loopback-packets`**

Example

```
OS900(config-efm)# discard-loopback-packets
OS900(config-efm)#
```

***Disabling Discarding of Packets Looped Back via BO***

To disable packets that are looped back via the BO from being discarded, invoke the command:

**`no discard-loopback-packets`**

Example

```
OS900(config-efm)# no discard-loopback-packets
OS900(config-efm)#
```

**BO**

***Resetting an OESD***

To reset an OESD (EM316GRMAHSH or EM316EFRMAHSH), invoke the command:

**`rm mrv reset warm|cold loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the BO.

**`warm`** Warm reset (restart *without* powering off) the BO.

**`cold`** Cold reset (restart *with* powering off) the BO.

Example

```
OS900(config-efm)# rm mrv reset warm loc-port 5
OS900(config-efm)#
```

***Setting OESD Port Speed***

To set the speed of an OESD port, invoke the command:

**`rm mrv config loc-port PORT rm-port p# speed 10|100|1000`**

where,

**`PORT`** OS900 port that is connected to the BO.

**`p#`** Port of BO that is connected to an OS900 port:

**`10`** 10 Mbps.

**`100`** 100 Mbps.

**`1000`** 1000 Mbps.

Example

```
OS900(config-efm)# rm mrv config loc-port 6 rm-port p4 speed 100
OS900(config-efm)#
```

### *Setting OESD Port Duplexity*

To set the duplexity of a port of an OESD port, invoke the command:

**`rm mrv config loc-port PORT rm-port p# duplex half|full`**

where,

**`PORT`** OS900 port that is connected to the OESD.

**`p#`** OESD port that is connected to the OS900.

**`half`** Half-duplex mode.

**`full`** Full-duplex mode.

Example

```
OS900(config-efm)# rm mrv config loc-port 6 rm-port p4 duplex full
OS900(config-efm)#
```

### *Enabling/Disabling Auto-negotiation on an OESD Port*

To enable/disable auto-negotiation on a port of an OESD port, invoke the command:

**`rm mrv config loc-port PORT rm-port p# aneg off|on`**

where,

**`PORT`** OS900 port that is connected to the OESD.

**`p#`** OESD port that is connected to the OS900:

**`off`** Disable auto-negotiation.

**`full`** Enable auto-negotiation.

Example

```
OS900(config-efm)# rm mrv config loc-port 5 rm-port p4 aneg off
OS900(config-efm)#
```

### *Configuring Auto-negotiation Functions on an OESD Port*

To configure auto-negotiation functions on a port of an OESD port, invoke the command:

**`rm mrv config loc-port PORT rm-port p# aneg-caps`**

where,

**`PORT`** OS900 port that is connected to the OESD.

**`p#`** OESD port that is connected to the OS900.

Example

```
OS900(config-efm)# rm mrv config loc-port 8 rm-port p3 aneg-caps
Parameters: 1000Mbps, Full Duplex (y|n) :
y
Parameters: 100Mbps, Full Duplex (y|n) :
y
Parameters: 100Mbps, Half Duplex (y|n) :
y
Parameters: 10Mbps, Full Duplex (y|n) :
y
Parameters: 10Mbps, Half Duplex (y|n) :
OS900(config-efm)#
```

### *Activating a Specific Trunk Port of an OESD*

This command is applicable for a 'redundant trunk connection[54]' as well as for a 'dual-homing connection[55].'

To activate a specific *trunk* port of an OESD, invoke the command:

**`rm mrv config loc-port PORT active-trunk p1|p2|no-preference`**

where,

**`PORT`** OS900 port that is connected to the BO.

**`p1`** Port 1 of BO that is connected to local port.

[54] In redundant trunk connection, two trunk ports are connected to *the same* device.

[55] In dual-homing connection, two trunk ports are connected to *two different* devices.

**p2** Port 2 of BO that is connected to local port.

**no-preference** Don't care which of ports 1 and 2 of the BO is activated.

Example

```
OS900(config-efm)# rm mrv config loc-port 7 active-trunk p2
OS900(config-efm)#
```

### *Naming a BO*

To give a name to a *BO*, invoke the command:

**rm config loc-port PORT cpe-name WORD**

where,

**PORT** OS900 port that is connected to the BO.

**WORD** Name for the BO that is connected to local the port.

Example

```
OS900(config-efm)# rm config loc-port 7 cpe-name Tarzan
OS900(config-efm)#
```

The name of the *BO* is known only to the OS900. It is not known to the *BO*.

### *Deleting the name of a BO*

To delete the name of a *BO*, invoke the command:

**no rm config loc-port PORT cpe-name**

where,

**PORT** OS900 port that is connected to the BO.

Example

```
OS900(config-efm)# no rm config loc-port 7 cpe-name Tarzan
OS900(config-efm)#
```

### *Activating Flow Control on an OESD*

To activate IEEE 802.3x Flow Control on an OESD, invoke the command:

**rm mrv config loc-port PORT flow-control off|on**

where,

**PORT** OS900 port that is connected to the OESD.

**off** Disable Flow Control for the OESD.

**on** Enable Flow Control for the OESD.

Example

```
OS900(config-efm)# rm mrv config loc-port 12 flow-control on
OS900(config-efm)#
```

### *Setting Rate-limit on an OESD*

To set a rate-limit on an OESD, invoke the command:

**rm mrv config loc-port PORT rate-limit NUMBER**

where,

**PORT** OS900 port that is connected to the OESD.

**NUMBER** Number designating the rate-limit for the OESD. The unit for the rate-limit can be Kbps or Mbps. The OESD selects the unit automatically. For the OESDs EMR316EFRMAHSH and EM316GRMAHSH, select 1. EMR316EFRMAHSH will select the unit Kbps. EM316GRMAHSH will select the unit Mbps.

Example

```
OS900(config-efm)# rm mrv config loc-port 11 rate-limit 50
OS900(config-efm)#
```

### *Enabling a Port on an OESD*

To enable a port on an OESD, invoke the command:

**rm mrv config loc-port PORT rm-port p3|p4 enable on|off**

where,

**PORT** OS900 port that is connected to the OESD.

**p3** User port P3 of the OESD. (P3 is connected to the CE.)

**p4** User port P4 of the OESD. (P4 is connected to the CE.)

**on** Enable port.

**off** Disable port.

Example

```
OS900(config-efm)# rm mrv config loc-port 7 rm-port p3 enable on
OS900(config-efm)#
```

### *Auto-sense a Port on an OESD*

To set a port on an OESD to operate in auto-sense mode, invoke the command:

**rm mrv config loc-port PORT rm-port p4 auto-sense [off|on]**

where,

**PORT** OS900 port that is connected to the OESD.

**P4** User port P4 of the OESD. P4 is connected to the CE.

**on** Force mode[56].

**off** Auto-sense mode[57]. (Default)

Example

```
OS900(config-efm)# rm mrv config loc-port 21 rm-port p4 auto-sense on
OS900(config-efm)#
```

### *MDI/MDIX Setting for a Port on an OESD*

To set a port on an OESD to operate as either an MDI or MDIX interface, invoke the command:

**rm mrv config loc-port PORT rm-port p4 mdi-mode [mdi-x|mdi]**

where,

**PORT** OS900 port that is connected to the OESD.

**P4** User port P4 of the OESD. (P4 is connected to the CE.)

**mdi-x** MDIX interface. Pinout: 1 → Rx+, 2 → Rx-, 3 → Tx+, 6 → Tx-. (Default)

**mdi** MDI interface. Pinout: 1 → Tx+, 2 → Tx-, 3 → Rx+, 6 → Rx-.

Example

```
OS900(config-efm)# rm mrv config loc-port 5 rm-port p4 mdi-mode mdi
OS900(config-efm)#
```

### *Enabling Dual-homing for a Port on an OESD*

To enable a port on an OESD to operate in 'dual-homing' or 'redundant trunk connection' mode, invoke the command:

**mrv dual-home loc-port PORTS-GROUP|all**

where,

**PORTS-GROUP** Group of OS900 ports that is to be set to operate in 'dual-homing' or 'redundant trunk connection' mode.

**all** All ports to be set to operate in 'dual-homing' or 'redundant trunk connection' mode.

Example

```
OS900(config-efm)# mrv dual-home loc-port 1-6
OS900(config-efm)#
```

[56] The port speed is fixed.

[57] The Ethernet port sets its speed (10 or 100 Mbps) to match that of the port to which it is directly connected (provided the latter port too has auto-sensing capability).

### *Disabling Dual-homing for a Port on an OESD*

To disable a port on an OESD from operating in 'dual-homing' or 'redundant trunk connection' mode, invoke the command:

**`no mrv dual-home loc-port PORTS-GROUP|all`**

where,

**`PORTS-GROUP`** Group of OS900 ports that is to be disabled from operating in 'dual-homing' or 'redundant trunk connection' mode.

**`all`** All ports to be disabled from operating in 'dual-homing' or 'redundant trunk connection' mode.

Example

```
OS900(config-efm)# no mrv dual-home loc-port 8-11
OS900(config-efm)#
```

### *Clearing OAM Statistical Data on an OESD Port*

To clear OAM statistical data on an OESD port, invoke the command:

**`mrv clear oam-statistics loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the BO.

Example

```
OS900(config-efm)# clear oam-statistics loc-port 9
OS900(config-efm)#
```

### *Clearing General Statistical Data on a BO Port*

To clear general statistical data on an OESD port, invoke the command:

**`mrv clear phy-statistics loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the BO.

Example

```
OS900(config-efm)# clear phy-statistics loc-port 6
OS900(config-efm)#
```

### *Deleting File Containing the OESD Image*

To delete the file containing the image of the BO, invoke the command:

**`remove rm mrv sw-version-file FILENAME`**

where,

**`FILENAME`** Name of file containing the image of the BO.

Example

```
OS900(config-efm)# clear phy-statistics loc-port 6
OS900(config-efm)#
```

### *Traps*

Custom

To set the number of OAMPDUs each incorporating a dying gasp critical link event that are to be sent from the BO:

1. Enter **`configure terminal`** mode. (This can be done from **`configure terminal`** mode.)
2. Invoke the command:

   **`dying-gasp-trap <1-30>`**

   where,

   **`<1-30>`**: Number of OAMPDUs each incorporating a dying gasp critical link event.

Example

```
OS900(config)# dying-gasp-trap 4
OS900(config)#
```

Default

To set the number of dying gasp traps (to be sent) to the default value (5 traps):

1. Enter **efm** mode.
2. Invoke the command:

   **dying-gasp-trap default**

Example

```
OS900(config)# dying-gasp-trap default
OS900(config)#
```

## Viewing OAM Status

### CO

***Viewing OAM-enabled Ports***

To view OS900 ports that are OAM enabled, invoke the command:

**show ports PORTS-GROUP|all**

where,

**PORTS-GROUP** Group of OAM-enabled ports.

**all** All OAM-enabled ports.

Example

```
OS900(config-efm)# show ports all
Ports Enable = 3-7;
Ports Active = No;
OS900(config-efm)#
```

In the example above, ports 3 to 7 are OAM enabled. They are specified '`No`' (i.e., not active) because the OAM protocol on the OS900 has not been enabled (by the user).

***Viewing OAM Status of a* Local *Port***

To view the OAM status of an OS900 port, invoke the command:

**show oam-config loc-port PORT**

where,

**PORT** OS900 port that is connected to the target (remote) OAM device.

Example

Viewing the OAM status of an OS900 *port connected to a BO*:

```
OS900(config-efm)# show oam-config loc-port 9 target-device local
Oam Configuration Remote Device (on port 9)
----------------------------------------------
Revision            : 0
Vendor OUI          : 201a
Vendor Info         : 0
Max PDU Size        : 482 bytes
Mux Action          : 0 (FWD)
Parser Action       : 0 (FWD)
Discovery State     : SEND_ANY (6)
PDU State           : ANY (3)
Local Flags         : 0x50 (Discovery process has completed)
OS900(config-efm)#
```

The configuration parameters (shown in the example above) and their possible values are described below:

`Revision` The value of the Revision field in the Local Information TLV of the most recently *transmitted* Information OAMPDU.

`Vendor OUI` The value of the OUI variable in the Vendor Identifier field of the most recently received Information OAMPDU.

`0` Vendor-specific device not present.

`1` Vendor-specific device present.

`Vendor Info` The value of the Vendor Specific Information field of the most recently received Information OAMPDU.

`Max PDU Size` The largest OAMPDU supported by the OS900

`Mux Action` Action performed by multiplexer.

`FWD` Device is forwarding non-OAMPDUs to the lower sublayer.

`DISCARD` Device is discarding non-OAMPDUs.

`Parser Action` Action performed by frame-syntax analyzer.

`FWD` Device is forwarding non-OAMPDUs to higher sublayer.

`LB` Device is looping back non-OAMPDUs to the lower sublayer.

`DISCARD` Device is discarding non-OAMPDUs.

`Discovery State` The current state of the OAM discovery function.

`SEND_ANY` Normal operating state for OAM on fully operational links.

`FAULT` Link fault detected at local OS900.

`ACTIVE_SEND_LOCAL` Sending Information OAMPDUs that only contain the Local Information TLV.

`PASSIVE_WAIT` Waiting to receive Information OAMPDUs with Local Information TLVs before sending any Information OAMPDUs with Local Information TLVs.

`send local remote` Sending Information OAMPDUs that contain both the Local and Remote Information TLVs.

`send local remote ok` Local OAM client deems the settings on both the local and remote DTEs are acceptable.

`PDU State` Governing transmission and reception of OAMPDUs as part of the Discovery process[58].

`ANY` Any permissible OAMPDU is allowed to be transmitted and received.

`INFO` Only Information OAMPDUs are allowed to be transmitted and received.

LF_INFO Only Information OAMPDUs with the Link Fault critical link event set and without Information TLVs are allowed to be transmitted; only Information OAMPDUs are allowed to be received.

RX_INFO No OAMPDUs are allowed to be transmitted; only Information OAMPDUs are allowed to be received.

`Local Flags` 2-digit hex code indicating operation status as indicated in the most recently *transmitted* OAMPDU. The hex code translates into a 7-digit binary code. The first (LSB) bit in the binary code corresponds to the Link Fault bit in the Flags field. The second bit corresponds to the Dying Gasp[59] bit in the Flags field. The third bit corresponds to the Critical Event bit in the Flags field. The fourth bit corresponds to the Local Evaluating bit in the Flags field. The fifth bit corresponds to the Local Stable bit in the Flags field. The sixth bit corresponds to the Remote Evaluating bit in the Flags field. The seventh (MSB) bit corresponds to the Remote Stable bit in the Flags field.

The significance of the value of each bit is given in *Table 17*, below.

[58] Checking if the IEEE 802.3ah and ITU-T Y.1731 parameter values of the CO and CPE match.

[59] Indication of time to failure due to power outage.

### Table 17: Local Flag Bits – Values and Significances

| Bits | Flags | Values | Significances |
|---|---|---|---|
| 1 (LSB) | Link Fault | 0 | Link fault condition does exist. |
| | | 1 | Link fault condition does *not* exist. |
| 2 | Dying Gasp | 0 | An unrecoverable local failure condition has *not* occurred. |
| | | 1 | An unrecoverable local failure condition has occurred. |
| 3 | Critical Event | 0 | A critical event condition has *not* occurred. |
| | | 1 | A critical event condition has occurred. |
| 4 | Local Evaluating | 0 | Local DTE Discovery process has *not* completed. |
| | | 1 | Local DTE Discovery process has completed. |
| 5 | Local Stable | 0 | Local DTE either has not seen or is unsatisfied with remote state information. |
| | | 1 | Local DTE has seen and is satisfied with remote state information. |
| 6 | Remote Evaluating | 0 | Remote DTE Discovery process has *not* completed. |
| | | 1 | Remote DTE Discovery process has completed. |
| 7 (MSB) | Remote Stable | 0 | Remote DTE either has not seen or is unsatisfied with local state information. |
| | | 1 | Remote DTE has seen and is satisfied with local state information. |

In the above example, the 2-digit hex code 0x50 translates into the 7-digit binary code 101 0000.

Bit 5 is 1, indicating that local DTE has seen and is satisfied with *remote* state information.

Bit 7 is 1, indicating that the remote DTE has seen and is satisfied with *local* state information.

Example

To view the OAM status of an OS900 *port unconnected to a BO but on which the OAM protocol is enabled*:

```
OS900(config-efm)# show oam-config loc-port 5 target-device local
Oam Configuration Remote Device (on port 5)
----------------------------------------------
Revision             : 0
Vendor OUI           : 201a
Vendor Info          : 0
Max PDU Size         : 482 bytes
Mux Action           : 0 (FWD)
Parser Action        : 0 (FWD)
Discovery State      : ACTIVE_SEND_LOCAL (2)
PDU State            : INFO (2)
Local Flags          : 0x8 (Discovery process has not completed)
OS900(config-efm)#
```

***Viewing CO Ports***

To view which ports of an OS900 are CO ports, invoke the command:

**show rm table (PORTS-GROUP|all)**

where,

**PORTS-GROUP** Group of OAM-enabled ports.

**all** All OAM-enabled ports.

Example

```
OS900(config-efm)# show rm table 3
PORT STATE DISCOVERY-STATE MODULE-TYPE       CPE-NAME     RED-STAT RED-PORT
---------------------------------------------------------------------------
 3    En   ACTIVE_SEND_LOC                  CPE-3
OS900(config-efm)#
```

**BO**

### *Viewing OAM Status of an* OESD

To view the OAM status of an OESD that is connected to an OS900 port, invoke the command:

**show oam-config loc-port PORT target-device remote**

where,

**PORT** OS900 port that is connected to the target (remote) OAM device.

Example

```
OS900(config-efm)# show oam-config loc-port 8 target-device remote
Oam Configuration Remote Device (on port 8)
----------------------------------------------
Revision           : 0
Vendor OUI         : 201a
Vendor Info        : 220020
Max PDU Size       : 498 bytes
Mux Action         : 0 (FWD)
Parser Action      : 0 (FWD)
Remote Flags       : 0x50 (Discovery process has completed)
Loopback Ctrl      : Loopback Disabled (0)
LIN Ctrl           : Available, Disable
OS900(config-efm)#
```

`Revision` The value of the Revision field in the Local Information TLV of the most recently *transmitted* Information OAMPDU.

`Vendor OUI` The value of the OUI variable in the Vendor Identifier field of the most recently received Information OAMPDU.

- `0` Vendor-specific device not present.
- `1` Vendor-specific device present.

`Vendor Info` The value of the Vendor Specific Information field (see Table 57–11) of the most recently received Information OAMPDU.

`Max PDU Size` `The largest OAMPDU supported by the OS900`

`Mux Action` Action performed by multiplexer.

- `FWD` Device is forwarding non-OAMPDUs to the lower sublayer.
- `DISCARD` Device is discarding non-OAMPDUs.

`Parser Action` Action performed by frame-syntax analyzer.

- `FWD` Device is forwarding non-OAMPDUs to higher sublayer.
- `LB` Device is looping back non-OAMPDUs to the lower sublayer.
- `DISCARD` Device is discarding non-OAMPDUs.

`Remote Flags` 2-digit hex code indicating operation status as indicated in the most recently *received* OAMPDU. The hex code translates into a 7-digit binary code. The first (LSB) bit in the binary code corresponds to the Link Fault bit in the Flags field. The second bit corresponds to the Dying Gasp bit in the Flags field. The third bit corresponds to the Critical Event bit in the Flags field. The fourth bit corresponds to the Local Evaluating bit in the Flags field. The fifth bit corresponds to the Local Stable bit in the Flags field. The sixth bit corresponds to the Remote Evaluating bit in the Flags field. The seventh (MSB) bit corresponds to the Remote Stable bit in the Flags field.

The significance of the value of each bit is given in *Table 17*, page *436*.

`Loopback Ctrl` Loopback control status.

`LIN Ctrl` Link Integrity Notification control status.

### *Viewing General Information on an OESD*

To view the general information on an OESD that is connected to an OS900 port, invoke the command:

**show rm mrv general-status loc-port PORT**

where,

**PORT** OS900 port that is connected to the target (remote) device.

Example

```
OS900(config-efm)# show rm mrv general-status loc-port 8
boardId            : 19 (0x13) EM316-GRMAHSH (subid 0)
macAddress         : 00:20:1a:02:0d:15
appRev             : MRViw-5.00 (0020)
```

```
fpgaRev             : 73.03
preamble            : disabled
packetMode          : enabled
CO State            : This is not a CO.
dipSwitch           : (0x0022)
  MDIX ANEG 1000 100M HDLX CPE  LIN  RM   MGMT LPBK PMBL
  DIS                                DIS  DIS
  off  on   off  off  off  on   off  off  off  off  off
OS900(config-efm)#
```

### *Viewing Port Status of an OESD*

To view the status of an OESD port, invoke the command:

**`show rm mrv interface-status loc-port PORT rm-port p#`**

where,

**`PORT`** OS900 port that is connected to the OESD.

**`p#`** OESD port:

Example

```
OS900(config-efm)#



---------------------------------FOR SFP PORT (p1)--------------------------------

OS900(config-efm)# show rm mrv interface-status loc-port 14 rm-port p1
Interface Status of port p1 (remote) is connected to port 14 (local)
--------------------------------------------------------------------------
ifType              : Ethernet (6)
ifLogType           : trunk
ifLink              : up
ifTrunkState        : prim
ifDuplex            : full
ifAutoNeg           : on
ifPhyType           : FiberOptic
ifAdminSpeed        : 100Mbs
ifSpeed             : 100Mbs
SFP Present         : present
Port Status         : active
ifPhy Detail Type   : SFP Port

   SFP Vendor Information
   *************************************
Identifier is XFF
Connector code is LC
Transciever subcode is 100Base-FX
Serial encoding mechanism is NRZ
The nominal bit rate is 200 Megabits/sec.
Link length using single mode (9 micron) is not supported.
Link length using 50 micron multi-mode fiber is greater than 2000m.
Link length using 62.5 micron multi-mode fiber is greater than 2000m.
Link length using cooper cable is not supported.
Vendor name is AGILENT
Vendor PN is HFBR-57E0P
Vendor revision is
Nominal transmitter output wavelength at room temperature is 1310.00 nm.
======================================================================

OS900(config-efm)#



-------------------------------FOR COPPER port (P4)-------------------------------

OS900(config-efm)# show rm mrv interface-status loc-port 14 rm-port p4
```

```
Interface Status of port p4 (remote) is connected to port 14 (local)
--------------------------------------------------------------------------
ifType              : Ethernet (6)
ifLogType           : user
ifLink              : down
ifDuplex            : half
ifAutoNeg           : off
ifPhyType           : Copper
ifAdminSpeed        : 100Mbs
ifSpeed             : 10Mbs
Port Status         : active
ifPhy Detail Type   : RJ-45 Port
Advertises the Following Auto-Negotiation Capabilities:
                     100Mbps, Full Duplex
                     100Mbps, Half Duplex
                      10Mbps, Full Duplex
                      10Mbps, Half Duplex
OS900(config-efm)#
```

***Viewing OAM Statistics on a* BO *Port***

To view the OAM statistics on a port of an OESD, invoke the command:

**`show loc oam-statistics loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the BO.

<u>Example</u>

```
OS900(config-efm)# show rm mrv oam-statistics loc-port 1
OAM statistics for target that is connected to local port 1.
-----------------------------------------------------------------------
OAM COUNTS          :        TX           RX
Information         :     22368         4609
EventNotify         :         0            0 (unique)
                    :         0            0 (duplicate)
Loopback            :         0            0
VarRequest          :         0            0
VarResponse         :         0            0
OrgSpecific         :     26595           10
Unsupported         :         0            0

Total               :     48963         4622

NON-OAM LOOPBACK    :    COUNTS BAD FRAMES
sent                :         0 nBadSubtype         :         0
echo                :         0 nBadVersion         :         0
drop                :         0 nFramesLost         :         0
rcvd                :         0
discard             :         0

locFlags            :0x50
remFlags            :0x50
locSA               :00:20:1a:02:0d:15
remSA               :00:20:1a:02:0d:15
OS900(config-efm)#
```

***Viewing General Statistics on an* OESD *Port***

To view the general statistics on a port of an OESD, invoke the command:

**`show rm mrv phy-statistics loc-port PORT rm-port-type trunk|user`**

where,

**`PORT`** OS900 port that is connected to the BO.

**`trunk`** Port P1 or P2 of the OESD. (P1 and P2 are connected to the OS900.)

**`user`** Port P3 or P4 of the OESD. (P3 and P4 are connected to the CE.)

Example

```
OS900(config-efm)# show rm mrv phy-statistics loc-port 1 rm-port-type trunk
MAC Layer statistics for trunk port (connected to local port 1.)
--------------------------------------------------------------------------
InOctets            :    309632     OutOctets                :   3557377
InUcastPkts         :         1     OutUcastPkts             :         0
InMcastPkts         :      4837     OutMcastPkts             :     49620
InBroadcastPkts  :   0   OutBroadcastPkts     :    0
InPausePkts         :         0     OutPausePkts             :         0
InDiscards          :         0     OutDiscards              :         0
InFCSErrs           :         0     OutDeferreds             :         0
InAlignmentErrs     :         0     OutSingleCollision       :         0
InUndersize         :         0     OutMultipleCollision     :         0
InRxOversize        :         0     OutLateCollision         :         0
InJabbers           :         0     OutExcessiveCollision    :         0
Duplex              :      full
Transmit            :   enabled
Multicast Receive   :   enabled
Unicast Addr        :00:20:1a:02:0d:15
OS900(config-efm)#
```

***Viewing Standard Mandatory Counters and Parameters on a* BO**

To view the standard *mandatory* counters and parameters of a *BO*, invoke the command:

**`show rm package mandatory loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the BO.

Example

```
OS900(config-efm)# show rm package mandatory loc-port 1
Variables Mandatory Package for target that is connected to local port 1.
--------------------------------------------------------------------------
aFramesTransmittedOK          :     52621
aSingleCollisionFrames        :         0
aMultipleCollisionFrames      :         0
aFramesReceivedOK             :      5706
aFrameCheckSequenceErrors     :         0
aAlignmentErrors              :         0
aDuplexStatus                 :      full
OS900(config-efm)#
```

***Viewing Standard Optional Counters and Parameters on a* BO**

To view the standard *optional* counters and parameters of a *BO*, invoke the command:

**`show rm package optional loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the BO.

Example

```
OS900(config-efm)# show rm package optional loc-port 1
Variables Optional Package for target that is connected to local port 1.
--------------------------------------------------------------------------
aMulticastFramesXmittedOK          :     53302
aBroadcastFramesXmittedOK          :         0
aMulticastFramesReceivedOK         :      5904
aBroadcastFramesReceivedOK         :         0
aInRangeLengthErrors               :         0
aFrameTooLongErrors                :         0
aMACEnableStatus                   :   enabled
aTransmitEnableStatus              :   enabled
aMulticastReceiveStatus            :   enabled
aReadWriteMACAddress               : 00:20:1a:02:0d:15
OS900(config-efm)#
```

### *Viewing Standard Recommended Counters and Parameters on a* BO

To view the standard *recommended* counters and parameters of a *BO*, invoke the command:

**show rm package recommended loc-port PORT**

where,

**PORT** OS900 port that is connected to the BO.

Example

```
OS900(config-efm)# show rm package recommended loc-port 1
Variables Recommended Package for target that is connected to local port 1.
---------------------------------------------------------------------------
aOctetsTransmittedOK               :   3848716
aFramesWithDeferredXmissions       :         0
aLateCollisions                    :         0
aFramesAbortedDueToXSColls         :         0
aFramesLostDueToIntMACXmitErrs     :         0
aCarrierSenseErrors                :         0
aOctetsReceivedOK                  :    385600
aFramesLostDueToIntMACRcvErrs      :         0
aPromiscuousStatus                 :         1
OS900(config-efm)#
```

### *Viewing Number of Dying Gasp OAMPDUs*

To view the number of OAMPDUs each incorporating a dying gasp critical link event set for sending:

1. Enter **enable** mode.
2. Invoke the command:

   **show efm-cpe dying-gasp-trap**

Example

```
OS900# show efm-cpe dying-gasp-trap
Number of dying-gasp alarms (traps) to be send is 4
OS900#
```

# Events

The OAM in the OS900 can be set to send notifications on events of the following types:

**critical-link** Critical events (e.g., remote device is powered off).

**regular-link** Errored Symbol Period Event and Errored Frame Event.

**user-port-link** Link-state change on the port of an OESD. The possible states are Up and Down.

When an event occurs, notification is sent to all open CLI sessions as well as to the Syslog.

### *Disabling Event Notification*

To disable event notification, invoke the command:

**no event-notification mode**

Example

```
OS900(config-efm)# no event-notification mode
OS900(config-efm)#
```

### *Enabling Event Notification*

By default, event notification is enabled for all the three event types specified above.

In any case, to enable event notification, invoke the command:

**event-notification more critical-link|regular-link|user-port-link|all**

where,

**critical-link** Critical link events. They include the following subtypes:

***Link Fault*** The PHY layer has determined that a fault has occurred in the receive direction of the local DTE.

***Dying Gasp*** An unrecoverable local failure condition has occurred (e.g., remote device is powered off).

***Critical Event*** An unspecified critical event has occurred.

**`regular-link`** Errored Symbol Period and Errored Frame events.

**`user-port-link`** Link-state change on the port of an OESD. The possible states are Up and Down.

**`all`** All event types.

Example

```
OS900(config-efm)# event-notification mode all
OS900(config-efm)#
```

Following are examples of the event notifications sent to a CLI-session form an OESD:

```
OS900(config-efm)# EFM event: User port on the CPE (connected to the local port 8) Link
State Changed => Up.

OS900(config-efm)# EFM event: User port on the CPE (connected to the local port 8) Link
State Changed => Down.

OS900(config-efm)# Event: EFM event "DyingGasp" is received on the port 8.
```

The '`DyingGasp`' event notification was the result of a power cut to a BO.

***Viewing Event Statistics***

To view OAM event statistics, invoke the command:

**`show rm oam-events loc-port PORT`**

where,

**`PORT`** OS900 port.

Example

```
OS900(config-efm)# show rm oam-events loc-port 1
-------------------------------------------------------------------------
ErrEvnt| TimeStamp     Window  Threshold      Count        Total  EvntCnt
-------------------------------------------------------------------------
Symbol |         0          0          0          0            0        0
Frame  |         0          0          0          0            0        0
FrmPer |         0          0          0          0            0        0
FrmSumm|         0          0          0          0            0        0
Link   |                                                                 0
DyiGasp|                                                                 1
Critic |                                                                 0
OS900(config-efm)#
```

# Firmware Upgrade/Download to an OESD

## General

This section shows how to upgrade/download an image (operative firmware) to MRV OESDs. The upgrade/download can be performed concurrently to several OESDs with a single CLI command.

## Viewing Data on an OESD Image in an OESD

To view the data on the OESD image portions loaded into an OESD, invoke the command:

**`show rm mrv general-status loc-port PORT`**

where,

**`PORT`** OS900 port that is connected to the OESD.

Example

```
OS900(config-efm)# show rm mrv general-status loc-port 1
boardId            : 19 (0x13) EM316-GRMAHSH (subid 0)
macAddress         : 00:20:1a:02:0d:15
appRev             : MRViw-5.00 (0020)
fpgaRev            : 73.03
preamble           : disabled
packetMode         : enabled
CO State           : This is not a CO.
dipSwitch          : (0x0022)
  MDIX ANEG 1000 100M HDLX CPE  LIN  RM   MGMT LPBK PMBL
  DIS                                DIS  DIS
  off  on   off  off  off  on   off  off  off  off  off
OS900(config-efm)#
```

In the example above, the OESD image portions are: ‘`appRev` ‘ and ‘`fpgaRev` ‘.

## Viewing Data on an OESD Image in an OS900

At any time, only one OESD image can be stored on an OS900.

To view the download state and data on the OESD image portions stored on an OS900, invoke the command:

**`show rm mrv download-state`**

Example

```
OS900 (config-efm)# show rm mrv download-state
EM316GRMAHSH-CPE : AppFile - N, FpgaFile - N, VerFile - N, AppVer - , FpgaVer - .
EM316EFRMAHSH-CPE: AppFile - Y, FpgaFile - Y, VerFile - Y, AppVer - MRViw-5.00 (0034),
FpgaVer -93.00.
Remote download is not active on local ports.
OS900 (config-efm)#
```

The above example shows that no image portion exists for the EM316GRMAHSH OESD, and that download is not in process.

## Procedure

To download new firmware to one or more OESDs connected to an OS900:

1. Copy the image file from an FTP server to the OS900 connected to the OESDs by invoking the following CLI command at the OS900 console:

   **`copy mrv-em316-ver ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]`**

   **`copy mrv-os304-ver ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]`**

   where,

   **`mrv-em316-ver`** Image version for MRV EM316-AH modules.

   **`mrv-os304-ver`** Image version for MRV OS304 modules.

   **`FTP-SERVER`** IP address of the FTP server containing the image file.

   **`REMOTE-DIR`** Name of directory in the FTP server containing the image file.

   **`REMOTE-FILENAME`** Name of file (containing the image) in the directory.

   **`USERNAME`** Username for permission to access the FTP server.

   **`PASSWORD`** Password for permission to access the FTP server.

   When the file is copied to the OS900 it is split into the following three files:

   – Application (contains the image portions)

   – FPGA (contains the image portions)

   – Versions (contains version identifications in text format)

   These files are retained in the OS900 so long as the OS900 is not reset.

Example

```
OS900(config-efm)# copy mrv-em316-ver ftp 10.100.100.10 . ef-34.rev
```

```
sudo /usr/local/nbase/bin/copy_em316ver.sh 10.100.100.10 . ef-34.rev
Check route to 10.100.100.10
Netmask = 255.255.255.0
FTP file ./ef-34.rev from 10.100.100.10 user  password  ...
FTP Succeed
<-         eakapp.bin     215356 Thu Jun 15 22:04:39 2006 crc:0xba79db9e OK
<-         eakfpga.bin    234456 Thu Jun  1 21:35:06 2006 crc:0x4c8dcb0f OK
<-         eakvrsn        27 Thu Jun 15 22:09:05 2006 crc:0xf2a6ef7c OK
OS900(config-efm)#
```

'`eakapp.bin` ' is the Application file

'`eakfpga.bin` ' is the FPGA file

'`eakvrsn` ' is the Versions file.

2. Upgrade/download the image to the OESD(s) connected to the OS900 with the Application and FPGA files by invoking the following command:

   **`rm mrv sw-dnld loc-ports PORTS-GROUP|all`**

   where,

   **`PORTS-GROUP`** Group of ports of the OS900 to which are connected OESDs to be loaded with the new image.

   **`all`** OESDs at all ports of the OS900 to be loaded with the new image.

   During upgrade/download, the firmware portions in the Application and FPGA files are downloaded to the OESDs. Versions file is not downloaded. Its contents are for factory use.

<u>Example</u>

```
OS900(config-efm)# rm mrv sw-dnld loc-ports 21

OS900(config-efm)#
The download process of the remote CPE (port 21) started.
..................................................
The FPGA-image is transmitted to remote CPE successfully !
..............................................
The APP-image is transmitted to remote CPE successfully !

    NOTE:  The update version action on the remote CPE
           will take few minutes.
           Link and EFM-connections with remote CPE
           (port 21) will be lost during this time.

EFM event: local port 21: Connection between CO and CPE is down.
EFM event: local port 21: Connection between CO and CPE is up.

The APP-version and FPGA-version are updated
on the remote CPE (port 21) successfully !

The download process on all requered local ports are finished.

OS900(config-efm)#
```

## Failure Messages

In the event that the upgrade/download process fails, any one of the following messages described in *Table 18*, below, will appear:

**Table 18: Failure Messages and their Significances**

| No. | Message | Significance |
|---|---|---|
| 1 | ***Canceled: new SW version info don't accessible (for this OESD)!*** | The new image is not suitable for the specific type of the OESD. For instance, it may be that the remote OESD is an EM316***G***RMAHSH while the image on the OS900 is for an EMR316***EF***RMAHSH. |
| 2 | ***Canceled: new SW version is the same as on the remote OESD !*** | The new image in the OESD is identical to the image in the OS900 for the OESD. |
| 3 | ***Canceled: Discovery process on the local port is not completed !*** | Transfer of the image portions to the OESD has failed. A possible cause for the failure could be that a portion of the image in the OS900 is missing or defective. |
| 4 | ***Canceled: EFM is not active on the port - <PORT> !*** | The OAM protocol is disabled for the OS900 and/or the specific port. To enable the OAM protocol for the OS900, invoke the command as described in the section *Enabling OAM Protocol*, page *427*. To enable the OAM protocol for a specific port of the OS900, invoke the command as described in the section *Enabling Ports*, page *428*. |

# Chapter 23: Authentication, Authorization, and Accounting (AAA)

## General

The best way to allow management access (especially remote access) to the OS900 by multiple administrators is to have a *single* database of administrators and a service mechanism that can perform the following **AAA** functions with this database:

- **A**uthentication: **I**dentification of requester profile [username, password, and privilege level] on a per-request basis.
- **A**uthorization: Permission/denial of access to a subset of commands subject to authentication success/failure. (The mechanisms of Authorization and authentication are independent of each other.)
- **A**ccounting: Reporting of information on requesters (identities, number of access attempts per requester, start and stop times, executed commands, etc.)

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) and TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess-**C**ontrol **S**ystem) are such service mechanisms. Both RADIUS and TACACS+ are Layer 7 (Application Layer) protocols. This chapter compares them and shows how they can be used on the OS900.

## RADIUS versus TACACS+

*Table 19*, below, compares the AAA protocols RADIUS and TACACS+ run on the OS900.

**Table 19: RADIUS versus TACACS+**

| No. | RADIUS | TACACS+ |
|---|---|---|
| 1 | Industry standard. Complies with RFC 2865. | Cisco proprietary. Complies with RFC 1492. |
| 2 | UDP-based, offering best-effort delivery. Utilizes UDP Port 1812. | TCP-based, offering connection-oriented determinism. Utilizes TCP Port 49. |
| 3 | RADIUS UDP is simpler to implement. | TCP makes TACACS+ more scalable. |
| 4 | Combines Authentication and Authorization. | Separates Authentication from Authorization. |
| 5 | Encrypts only the password in the connection request packet. | Encrypts the whole connection request packet. |

## Principles of Operation

The OS900 acts as a Network Access Server (NAS) for requesters, and therefore functions as an AAA client passing requester information (e.g. username, password, etc.).

The AAA Server, on the other hand, is responsible for receiving requester connection requests, authenticating or disqualifying the requester, and sending the permit or deny response to the client OS900.

Transactions between the OS900 and the AAA Server are permitted by shared secrets, which are never sent over the network. In addition, every administrator password is encrypted before it is sent between the OS900 and the AAA Server in order to prevent deciphering.

The AAA Server can also provide accounting of requester commands and of changes in authorization level. This information is recorded in a special log file that enables a supervisor to view the activities of all the administrators. Accounting can include logging of commands or logging of transitions from one mode to another.

# Configuring the AAA Server

To configure an AAA Server[60] to communicate with an OS900, do the following:

1. At the AAA Server, configure the OS900 as a NAS.
2. Set up shared secrets. In particular, enter the same encryption/decryption key on the AAA Server as that entered (or to be entered) on the OS900.
3. If AAA is to mediate when an attempt is made to access the OS900 at **`login`** mode, log the username & associated password of each administrator.

   If AAA is to mediate when an attempt is made to access the OS900 at **`enable`** mode, log a username and password for **`enable`** mode. The default username to be logged at the AAA is *`$enab15$`*.

   If AAA is to mediate when an attempt is made to access the OS900 at **`configure terminal`** mode, log a username and password for **`configure terminal`** mode. The username logged at the AAA Server must be the username to be entered at the OS900 indexed with the string **`.config`**. For example, if the username to be entered at the OS900 is **`Jojo`**, the username logged at the AAA Server must be **`Jojo.config`**.

   If AAA is to mediate when an attempt is made to access the OS900 at **`debug`** mode, log a username and password for **`debug`** mode. The default username to be logged at the AAA is *`$debug$`*.

> **Note**
>
> To allow a user attempting to enter **`enable`** mode of the OS900 *immediately after*[61] successfully logging onto the OS900 using the admin password, set the 'Service Type' parameter on the AAA Server to the value 'administrative user.'

# Configuring the OS900

## General

To configure an OS900 to communicate with an AAA Server, the following need to be done:

1. Setting Authentication Criteria

   This includes:

   a. IP address/hostname of the AAA Server(s) that can be accessed by the OS900. (Currently, the IP address/hostname of up to 10 AAA Servers can be set.)
   b. Encryption/decryption key – global or per AAA Server. This is text shared between the OS900 and the AAA Server and is used to encrypt and decrypt messages.
   c. Timeout – (optional) Global or per AAA Server. This is the time the OS900 waits for a response from the AAA Server.
   d. Application port – (optional) Per AAA Server. This is the port used by the OS900 to access the AAA Server. For RADIUS it is UDP Port 1812. For TACACS+ it is TCP Port 49.
   e. If AAA is to be applied when an attempt is made to access the OS900 at **`enable`** mode, the username and password that are configured for *enable* mode should be configured on the AAA

[60] The AAA server may be the AAA server itself or a device via which the OS900 communicates with the AAA server.

[61] '*immediately after*' means without having to type the password required to enter **`enable`** mode.

Server.
If AAA is to be applied when an attempt is made to access the OS900 at **`debug`** mode, the username and password that are configured for *debug* mode should be configured on the Server.
On the OS900, only one username can be defined for **`enable`** mode, only one username can be defined for **`debug`** mode. Each of these usernames is generic, meaning that, administrators with different **`login`** usernames can access these modes. The default username for **`enable`** mode is *`$enab15$`*. The default username for **`debug`** mode is *`$debug$`*. This is so because the OS900 sends the generic username and not the **`login`** username to the Authentication Server.

2. Setting Authentication
3. Activating Accounting
4. Viewing Accounting

## Setting Authentication Criteria

To set the authentication criteria:

1. Enter **`configure terminal`** mode.
2. Several Server IP addresses/hostnames can be specified for AAA by invoking the same command repeatedly and/or different commands given in this step. For AAA, the OS900 will attempt to access the AAA Servers *in the order*[62] *in which they were specified* till it succeeds.

   To set authentication criteria for *specific* AAA Servers, invoke any one of the following commands:

   a. This command is used to specify the AAA Server IP address/hostname.

      **`radius-server host <A.B.C.D|HOSTNAME>`**

      Or

      **`tacacs-server host <A.B.C.D|HOSTNAME>`**

      where,

      **`A.B.C.D`**: IP address of the AAA Server

      **`HOSTNAME`**: DNS hostname

   b. This command is used to specify the AAA Server IP address/hostname and encryption/decryption key.

      **`radius-server host <A.B.C.D|HOSTNAME> key LINE`**

      Or

      **`tacacs-server host <A.B.C.D|HOSTNAME> key LINE`**

      where,

      **`A.B.C.D`**: IP address of the AAA Server

      **`LINE`**: Text of shared encryption key between the OS900 and the AAA Server. An unbroken string of printable characters[63] may be entered.
      For TACACS+ the string can be up to 100 characters long.
      For RADIUS the string can be up to 16 characters long.
      The default encryption/decryption key is **`testing123`**.

   c. This command is used to specify the AAA Server IP address/hostname, encryption/decryption key, and timeout.

      **`radius-server host <A.B.C.D|HOSTNAME> key LINE timeout NUMBER`**

      Or

[62] This order for servers can be viewed by invoking the command **`show running-config`** or **`write terminal`**.

[63] Printable characters an be viewed by clicking on the link http://en.wikipedia.org/wiki/File:ASCII_full.svg.

**tacacs-server host <A.B.C.D|HOSTNAME> key LINE timeout NUMBER**

where,

**A.B.C.D**: IP address of the AAA Server

**HOSTNAME**: DNS hostname

**LINE**: Text of shared encryption key between the OS900 and the AAA Server. Any alphanumeric unbroken string may be entered. The default encryption/decryption key is **testing123**.

**NUMBER**: Timeout time, i.e., the time (in seconds) the OS900 waits for a response from the AAA Server. If the AAA Server gives a negative response or if it does not a respond within this time, access to the OS900 is denied. The default timeout is **3** seconds.

d. This command is used to specify the AAA Server IP address/hostname and timeout. The default encryption/decryption key is **testing123**.

**radius-server host <A.B.C.D|HOSTNAME> timeout NUMBER**

Or

**tacacs-server host <A.B.C.D|HOSTNAME> timeout NUMBER**

where,

**A.B.C.D**: IP address of the AAA Server

**HOSTNAME**: DNS hostname

**NUMBER**: Timeout time, i.e., the time (in seconds) the OS900 waits for a response from the AAA Server. If the AAA Server gives a negative response or if it does not a respond within this time, access to the OS900 is denied. The default timeout is **3** seconds.

e. This command is used to specify the AAA Server IP address/hostname and application port. The default timeout is **3** seconds. The default encryption/decryption key is **testing123**.

**radius-server host <A.B.C.D|HOSTNAME> port PORT**

Or

**tacacs-server host <A.B.C.D|HOSTNAME> port PORT**

where,

**A.B.C.D**: IP address of AAA Server that can be accessed by the OS900.

**HOSTNAME**: DNS hostname

**PORT**: Application port (protocol or service) to be authenticated. The default for RADIUS is **1812**. The default for TACACS+ is **49**. To display the port numbers and associated services, enter linux mode (by first entering **enable** mode and then typing **linux**), type **/etc/services**.

(To cancel *a specific* AAA Server, invoke the command **no radius-server host <A.B.C.D|HOSTNAME>** or **no tacacs-server host <A.B.C.D|HOSTNAME>**, where **<A.B.C.D|HOSTNAME>** is the IP address/DNS hostname of the AAA Server.)

(To cancel *all* AAA Servers, invoke the command **no radius-server** or **no tacacs-server**.)

3. To allow AAA access to the OS900 **enable** mode by an authorized requester if a username other than the default (*$enab15$*) is to be used, invoke the command:

**radius-server enable user NAME**

Or

**tacacs-server enable user NAME**

where,

**enable**: Set the OS900 to request authentication from the AAA Server when an attempt is made to access the OS900 **enable** mode.

**NAME**: Username. This username must be the same as that on the AAA Server. When an attempt is made to access the OS900 at **enable** mode, the OS900 sends this username to the AAA Server. The AAA Server finds the associated password, which it sends to the OS900. The OS900 then prompts the requester to enter a password. Only if the passwords match, access is granted.

On the OS900, only one username can be defined for **enable** mode. This means that the same username must be configured on all AAA Servers if they are to provide their service to the OS900. This username is generic, meaning that, administrators with different **login** usernames can access this mode. This is so because the OS900 sends the generic username and not the **login** username to the AAA Server.

> **Note**
> Invocation of the command **radius-server enable user NAME** or **tacacs-server enable user NAME** is a prerequisite for the AAA-involving commands in step *4*, page *453*.

4. To allow AAA access to the OS900 **debug** mode by an authorized requester, invoke the command:

   **radius-server debug user NAME**

   Or

   **tacacs-server debug user NAME**

   where,

   **debug**: Set the OS900 to request authentication from the AAA Server when an attempt is made to access the OS900 at **debug** mode.

   **NAME**: Username. This username must be the same as that on the AAA Server. When an attempt is made to access the OS900 at **debug** mode, the OS900 sends this username to the AAA Server. The AAA Server finds the associated password, which it sends to the OS900. The OS900 then prompts the requester to enter a password. Only if both the username and password match, access is granted.

   On the OS900, only one username can be defined for **debug** mode. This means that the same username must be configured on all AAA Servers if they are to provide their service to the OS900. This username is generic, meaning that, administrators with different **login** usernames can access this mode. This is so because the OS900 sends the generic username and not the **login** username to the AAA Server.

> **Note**
> Invocation of the command **radius-server debug user NAME** or **tacacs-server debug user NAME** is a prerequisite for an AAA-involving command in step *6*, page *454*.

5. To set a common default key for all AAA Servers, invoke the command:

   **radius-server key LINE**

   Or

   **tacacs-server key LINE**

   where,

   **LINE**: Text of shared encryption key between the OS900 and any AAA Server. Any alphanumeric unbroken string may be entered. The default encryption/decryption key is **testing123**.

6. To cause the key configured with the **tacacs-server key LINE** command to appear encrypted on the CLI screen, invoke the command:

   **tacacs-server encrypt key**

   (To cancel appearance of encryption for the key on the CLI screen, invoke the command **no tacacs-server encrypt key**.)

7. To set a common default timeout for all AAA Servers, invoke the command:

**`radius-server timeout NUMBER`**

Or

**`tacacs-server timeout NUMBER`**

where,

**`NUMBER`**: Timeout time, i.e., the time (in seconds) the OS900 waits for a response from the AAA Server. If the AAA Server gives a negative response or if it does not a respond within this time, access to the OS900 is denied. The default timeout is **`3`** seconds.

## Setting Authentication

For each mode (**`login`**, **`enable`**, **`debug`** or **`configure terminal`**), any one of the following authentication options (prefixed by **`authentication`**) can be selected:

**`local`** Perform authentication locally and without AAA Server mediation, i.e., using only the login username and password stored in the OS900's memory. Since this is the default mode, it does not appear in the run-time configuration.

**`radius local`** Perform authentication with the RADIUS Server first. If no response is received from the RADIUS Server(s) within the timeout time, perform authentication using only the login username and password stored in the OS900's memory.

**`tacacs+ local`** Perform authentication with the TACACS+ Server(s) first. If no response is received from the TACACS+ Server within the timeout time, perform authentication using only the login username and password stored in the OS900's memory.

**`radius`** Perform authentication only with the RADIUS Server.
(Access to the OS900 is denied if the Server gives a negative response or if no response is received from the RADIUS Server within the timeout time.)

**`tacacs+`** Perform authentication only with TACACS+ Server.
(Access to the OS900 is denied if the Server gives a negative response or if no response is received from the TACACS+ Server within the timeout time.)

**`local radius`** Perform authentication using the login username and password as stored in the OS900's memory. If access fails, perform authentication with the RADIUS Server.

**`local tacacs+`** Perform authentication using the login username and password as stored in the OS900's memory. If access fails, perform authentication with the TACACS+ Server.

**`none`** Prevent login.

To set the authentication:

1. Enter **`configure terminal`** mode.
2. Enter **`aaa`** mode.
3. To cause the OS900 to "try to get a permit or deny response from an AAA Server first when an attempt is made to access the OS900 at **`login`** mode, and, if no response is received within the timeout time, perform authentication using the login username and password stored only in the OS900's memory", invoke the command:

   **`authentication login default radius local`**

   Or

   **`authentication login default tacacs+ local`**

**Note**

If there is no connection with the AAA server, the prompts '`Local login:`' and '`Local password:` ' appear for local (OS900) authentication of the access request.

To cause the OS900 to "try to get a permit or deny response from an AAA Server when an attempt is made to access the OS900 at **`login`** mode, and, if no response is received within the timeout time, deny access", invoke the command:

**`authentication login default radius`**

Or

**`authentication login default tacacs+`**

**WARNING!**

Before selecting the argument **`radius`** or **`tacacs+`**, ensure that the AAA Server is operational and that at least the following parameters are set correctly on the OS900: AAA Server IP address/hostname and encryption/decryption key.

You can make sure using the following safe method: Open a CLI session[64]. Enter **`configure terminal`** mode and invoke the command **`authentication login default radius`** or **`authentication login default tacacs+`**. Now attempt to open a TELNET session. This way, if the attempt fails (possibly because of an incorrect AAA parameter setting) access to the CLI agent is retained (via the CLI session) and any AAA parameter setting can be corrected in the CLI session.

To cause the OS900 to "prevent login", invoke the command:

**`authentication login default none`**

**WARNING!**

Invoking the command **`authentication login default none`** will lock the OS900, preventing any access to it.

4. To cause the OS900 to "try to get a permit or deny response from an AAA Server first when an attempt is made to access the OS900 at **`enable`** mode, and, if no response is received within the timeout time, perform authentication using the enable password stored only in the OS900's memory", invoke the command:

   **`authentication enable default radius local`**

   Or

   **`authentication enable default tacacs+ local`**

   To cause the OS900 to "try to get a permit or deny response from an AAA Server when an attempt is made to access the OS900 at **`enable`** mode, and, if no response is received within the timeout time, deny access", invoke the command:

   **`authentication enable default radius`**

   Or

   **`authentication enable default tacacs+`**

---

64 Using a serial/RS-232 connection.

**WARNING!**

Before selecting the argument **radius** or **tacacs+**, ensure that the AAA Server is operational and that at least the following parameters are set correctly on the OS900: AAA Server IP address/hostname and encryption/decryption key.

You can make sure using the following safe method: Open a CLI session. Enter **configure terminal** mode, then **aaa** mode, and invoke the command **authentication enable default radius** or **authentication enable default tacacs+**. Now attempt to open a TELNET session. This way, if the attempt fails (possibly because of an incorrect AAA parameter setting) access to the CLI agent is retained (via the CLI session) and any AAA parameter setting can be corrected in the CLI session.

It is recommended to set all AAA parameters from a "live" station (e.g., craft terminal or TELNET station) and to make all the access attempts via a second TELNET station. The purpose in this is to enable verification of parameter values accessible via an AAA server without exiting the "live" station.

5. To cause the OS900 to "try to get a permit or deny response from an AAA Server first when an attempt is made to access the OS900 at **configure terminal** mode, and, if no response is received within the timeout time, perform authentication using the configure terminal password stored only in the OS900's memory", invoke the command:

    **authentication configure default radius local**

    Or

    **authentication configure default tacacs+ local**

   To cause the OS900 to "try to get a permit or deny response from an AAA Server when an attempt is made to access the OS900 at **configure terminal** mode, and, if no response is received within the timeout time, deny access", invoke the command:

    **authentication configure default radius**

    Or

    **authentication configure default tacacs+**

**WARNING!**

Before selecting the argument **radius** or **tacacs+**, ensure that the AAA Server is operational and that at least the following parameters are set correctly on the OS900: AAA Server IP address/hostname, and encryption/decryption key.

You can make sure using the following safe method: Open a CLI session. Enter **configure terminal** mode and invoke the command **authentication configure default radius** or **authentication configure default tacacs+**. Now attempt to open a TELNET session. This way, if the attempt fails (possibly because of an incorrect AAA parameter setting) access to the CLI agent is retained (via the CLI session) and any AAA parameter setting can be corrected in the CLI session.

   To cause the OS900 to "prevent login", invoke the command:

    **authentication configure default none**

**WARNING!**

Invoking the command **authentication configure default none** will allow access to the OS900 without the need for entering the 'debug' mode password.

6. To cause the OS900 to "try to get a permit or deny response from an AAA Server first when an attempt is made to access the OS900 at **debug** mode, and, if no

response is received within the timeout time, perform authentication using the debug password stored only in the OS900's memory", invoke the command:

**`authentication debug default radius local`**

Or

**`authentication debug default tacacs+ local`**

To cause the OS900 to "try to get a permit or deny response from an AAA Server when an attempt is made to access the OS900 at **`debug`** mode, and, if no response is received within the timeout time, deny access", invoke the command:

**`authentication debug default radius`**

Or

**`authentication debug default tacacs+`**

**WARNING!**

Before selecting the argument **`radius`** or **`tacacs+`**, ensure that the AAA Server is operational and that at least the following parameters are set correctly on the OS900: AAA Server IP address/hostname, and encryption/decryption key.

You can make sure using the following safe method: Open a CLI session. Enter **`configure terminal`** mode and invoke the command **`authentication debug default radius`** or **`authentication debug default tacacs+`**. Now attempt to open a TELNET session. This way, if the attempt fails (possibly because of an incorrect AAA parameter setting) access to the CLI agent is retained (via the CLI session) and any AAA parameter setting can be corrected in the CLI session.

7. Specify the authentication method of the TACACS+ server, by invoking the command:

   **`tacacs-server [host (A.B.C.D|HOSTNAME)] authen-method (ascii-login|pap-ppp)`**

   where,

   **`[host (A.B.C.D|HOSTNAME)]`**: IP address or DNS hostname of the TACACS+Server. If this argument is omitted, the PAP PPP authentication method is used for all hosts for whom the authentication method has not been set.

   **`ascii-login`**: ASCII authentication method to be performed by TACACS+Server

   **`pap-ppp`**: PAP PPP authentication method to be performed by TACACS+Server. (Default)

To cause the OS900 to use the PAP PPP authentication method, invoke the command:

**`no tacacs-server [host (A.B.C.D|HOSTNAME)] authen-method`**:

where,

**`[host (A.B.C.D|HOSTNAME)]`**: IP address or DNS hostname of the TACACS+Server. If this argument is omitted, the PAP PPP authentication method is used for all hosts for whom the authentication method has not been set.

## Setting Authorization

To cause a TACACS+ server to restrict access to specific CLI commands in a specific mode, do the following:

On TACACS+ Server

Register the client data required by the TACACS+ server and the CLI commands that the client is authorized to access.

The first word comprising a CLI command is considered as the *name* and the remaining words as *arguments*. For example, in the command **`script NAME`**, the first word is **`script`** and is therefore the name while the argument is **`NAME`**.

In the negation of the command, which is **`no script NAME`**, the first word is **`no`** and is therefore the name while the arguments are **`script`** and **`NAME`**.

It is necessary to enter the CLI command at the TACACS+ server in full.

One way to determine whether the syntax in which a command is to be registered at the TACACS+ server(s) is to (at the OS900 CLI screen) enter the command name and successive arguments (if any) using the key ?.

Certain TACACS+ servers can be configured to restrict access per command or even to selective arguments and/or values of an argument.

The commands **`quit`**, **`exit`**, **`logout`**, and **`end`** are automatically authorized, i.e., they are *not* sent to the TACACS+ server for authorization.

If authorization is received for any of the modes **`login`**, **`enable`**, **`configure terminal`**, and **`debug`**, it extends to *all* commands in the mode as well as in all its submodes.

If authorization fails, the OS900 shows the syntax in which the command was supposed to be registered at the TACACS+ server in order to be able to get authorization for the command.

On OS900

1. Specify the TACACS+ server by invoking the command:

   **`tacacs-server host <A.B.C.D|HOSTNAME> key LINE`**

   where,

   **`A.B.C.D`**: IP address of the AAA Server

   **`HOSTNAME:`** DNS hostname

   **`LINE`**: Text of shared encryption key between the OS900 and the AAA Server. Any unbroken string of printable characters may be entered. The default encryption/decryption key (at the OS900) is **`testing123`**.

2. Enter `AAA` mode, and invoke the command:

   **`authorization login|enable|debug|configure tacacs+`**

   where,

   **`login`**: For authorizing access to CLI commands in *login* mode

   **`enable`**: For authorizing access to CLI commands in *enable* mode

   **`debug`**: For authorizing access to CLI commands in *debug* mode

   **`configure`**: For authorizing access to CLI commands in *configure terminal* mode

   (To cancel requirement for authorization, invoke the command **`no authorization login|enable|debug|configure`**.)

   At the AAA server, a command

## Accounting

### General

Accounting is the reporting of information (ID and activities) on requesters. The following information can be sent by the OS900 to the AAA or RADIUS Server:

- User (requester) name
- Date of access
- Time of access
- Accounting flags. If the command **`accounting exec radius|tacacs+`** (for activating accounting – see below) is executed, each start (login) and each stop (logout) is reported. If the command **`accounting commands radius|tacacs+`** is executed, each completion of a command execution is reported.
- Shell executions (service)

- NAS (OS900) IP address
- Commands invoked & executed

**Activating**

To activate accounting:

1. Enter **`configure terminal`** mode.
2. Enter **`aaa`** mode.
3. Invoke either of the following the commands:

   **`accounting exec radius|tacacs+`**

   where,

   **`exec`**: Shell execution actions (login/logout)
   **`radius`**: RADIUS protocol based
   **`tacacs+`**: TACACS+ protocol based
   Or

   **`accounting commands [login|enable|configure|debug] radius|tacacs+`**

   where,

   **`login`**: Login mode commands
   **`enable`**: Enable mode commands
   **`debug`**: Debug mode commands
   **`configure`**: Configure terminal mode commands
   **`radius`**: RADIUS protocol based
   **`tacacs+`**: TACACS+ protocol based

# Configuration Examples

For convenience, the parts of the configuration example are headed with a number (1, 2, etc.). The description of each part is given below:

- 1. Setting of AAA Server criteria: IP address, key, timeout.
- 2. Setting of application port (protocol or service) that will be common to all AAA Servers.
- 3. Setting the OS900 to request authentication from the AAA Server when an attempt is made to access the OS900 **`enable`**, **`debug`**, and **`configure terminal`** mode.
- 4. Setting the authentication.
- 5. Activating accounting.
- 6. Displaying configuration.
- 7. Saving configuration in permanent memory.

## RADIUS

```
MRV OptiSwitch 910 version d0907-21-07-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
1.
OS900(config)# radius-server host 193.85.1.67 key testing6789 timeout 5
2.
OS900(config)# radius-server host 193.85.1.67 port 3444
3.
OS900(config)# radius-server enable user TigerEnable
OS900(config)# radius-server debug user TigerDebug
4.
OS900(config-aaa)# authentication login default radius local
OS900(config-aaa)# authentication enable default radius local
OS900(config-aaa)# authentication configure default radius local
OS900(config-aaa)# authentication debug default radius
5.
OS900(config-aaa)# authorization login tacacs+
OS900(config-aaa)# authorization enable tacacs+
OS900(config-aaa)# authorization configure tacacs+
OS900(config-aaa)# authorization debug tacacs+
OS900(config-aaa)# accounting exec radius
6.
OS900(config-aaa)# write terminal
Building configuration...

Current configuration:
! version d0907-21-07-05
!
radius-server enable user TigerEnable
radius-server debug user TigerDebug
radius-server host 193.85.1.67 port 3444
radius-server host 193.85.1.67 key testing6789 timeout 5
!
aaa
 authentication login default radius local
 authentication enable default radius local
 authentication configure default radius local
 authentication debug default radius
 authorization login tacacs+
 authorization enable tacacs+
 authorization configure tacacs+
 authorization debug tacacs+
 accounting exec radius
7.
OS900(config-aaa)# write file
```

TACACS+

```
MRV OptiSwitch 910 version d0907-21-07-05
OS900 login: admin
Password:

OS900> enable
OS900# configure terminal
1.
OS900(config)# tacacs-server host 193.85.1.67 key testing6789 timeout 5
2.
OS900(config)# tacacs-server host 193.85.1.67 port 3444
3.
OS900(config)# tacacs-server enable user TigerEnable
OS900(config)# tacacs-server debug user TigerDebug
4.
OS900(config-aaa)# authentication login default local tacacs+
OS900(config-aaa)# authentication enable default local tacacs++
OS900(config-aaa)# authentication configure default local tacacs++
OS900(config-aaa)# authentication debug default tacacs+
5.
OS900(config-aaa)# accounting exec tacacs+
6.
OS900(config-aaa)# write terminal
Building configuration...

Current configuration:
! version d0907-21-07-05
!
tacacs-server enable user TigerEnable
tacacs-server debug user TigerDebug
tacacs-server host 193.85.1.67 port 3444
tacacs-server host 193.85.1.67 key testing6789 timeout 5
!
aaa
 authentication login default local tacacs+
 authentication enable default local tacacs+
 authentication configure default local tacacs++
 authentication debug default tacacs+
 accounting exec tacacs+
7.
OS900(config-aaa)# write file
```

# Chapter 24: IEEE 802.1X Access Control

## General

This chapter shows how to configure the OS900 so that it will perform authentication actions (on requests by clients through devices attached to its ports to connect to the OS900 network) before authorizing or rejecting connection.

Access to the OS900/network is port-based, i.e., if access is granted to just one client device attached to an IEEE 802.1X-enabled port it will be granted to the rest of the client devices attached to the same port.

## Purpose

IEEE 802.1X Access Control provides security against unauthorized attempts by clients to access the OS900 or its network.

## Requirements

### Authentication Server

The authentication server must be a RADIUS server.

### Client Devices

The client devices attached to an OS900 port must run IEEE 802.1X-complaint client software in order to be able to access the OS900/network. Such software is available, for example, with the Microsoft Windows Operating System XP.

## Interconnection

*Figure 42*, below, shows a typical interconnection of client devices, the OS900, and a RADIUS server for operation in the IEEE 802.1X protocol.

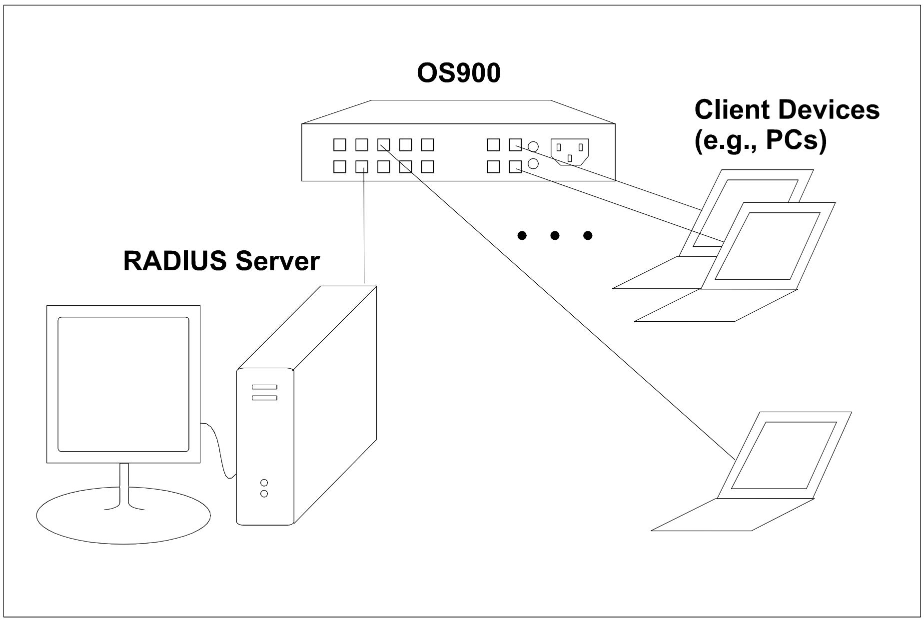



**Figure 42: IEEE 802.1X Access Control Network Interconnection**

# Configuration

## RADIUS Server

For configuration of a RADIUS Server, refer to the section *Configuring the AAA Server*, page *448*.

## OS900

Following is the procedure for basic configuration of the OS900 to operate in the IEEE 802.1X protocol. Additional configuration may be performed by changing the default values of the protocol parameters as described in the section *Optional Configuration Parameters*, page *462*.

1. From **configure terminal** mode, enter **dot1x** mode.
2. Enable the IEEE 802.1X protocol by invoking the command:
   **enable**
3. Specify the ports to operate in the IEEE 802.1X protocol (so that the RADIUS server controls accessibility for clients) by invoking the command:
   **port PORTS-GROUP mode auto**
   where,
   **PORTS-GROUP**: Group of ports.
   **auto**: Allow RADIUS server to perform authentication and to permit or deny access via the OS900 ports.

Example

```
OS910(config)# dot1x
OS910(config-dot1x)# enable
OS910(config-dot1x)# port 2-4 mode auto
OS910(config-dot1x)#
```

The example above shows that ports 2 to 4 have been configured to operate in the IEEE 802.1X protocol so that the RADIUS server controls accessibility for clients.

# Optional Configuration Parameters

## General

To change the values of the optional configuration parameters, first enter **dot1x** mode from **configure terminal** mode.

## Default Values

The default values of Optional Configuration Parameters are shown in *Table 20*, below.

**Table 20: Default Values of Optional Configuration Parameters**

| No. | Parameter | Default Value |
|---|---|---|
| 1 | IEEE 802.1X protocol<br>[Associated CLI command:<br>**enable**] | disabled |
| 2 | IEEE 802.1X protocol on port<br>[Associated CLI command:<br>**port PORTS-GROUP mode (auto\|force-auth\|force-unauth\|disable)**] | disabled |
| 3 | Maximum number of retransmissions of a request<br>[Associated CLI command:<br>**port PORTS-GROUP max-req <0-10>**] | 2 |
| 4 | Multiple client MACs per port<br>[Associated CLI command:<br>**port PORTS-GROUP multi-hosts (enable\|disable)**] | enabled |
| 5 | Time to wait for a reply from a server before retransmitting a packet | 30 seconds |

| | | |
|---|---|---|
| | [Associated CLI command: **port PORTS-GROUP server-timeout <1-65535>]** | |
| 6 | Time to wait following a failed authentication exchange with the client [Associated CLI command: **port PORTS-GROUP quiet-period <1-65535>]** | 60 seconds |
| 7 | Periodic reauthentication [Associated CLI command: **port PORTS-GROUP periodic-reauth enable [<1-65535>]]** | disabled |

## Enabling IEEE 802.1X Access Control Protocol

To enable the IEEE 802.1X Access Control Protocol, invoke the command:

**enable**

## Disabling IEEE 802.1X Access Control Protocol

To disable the IEEE 802.1X Access Control Protocol, invoke the command:

**no enable**

## Enabling RADIUS-Server-Controlled Accessibility

To *enable* one or more ports to operate in the IEEE 802.1X protocol so that the RADIUS server controls accessibility for clients, invoke the command:

**port PORTS-GROUP mode auto**

where,

**PORTS-GROUP**: Group of ports.

**auto**: Allow RADIUS server to perform authentication and to permit or deny access via the OS900 ports.

## Forcing Accessibility

To *enable* access to the OS900 via one or more of its ports regardless of the RADIUS server, invoke the command:

**port PORTS-GROUP mode force-auth**

where,

**PORTS-GROUP**: Group of ports.

**force-auth**: Allow access via the ports regardless of the RADIUS server.

## Forcing Inaccessibility

To *disable* access to the OS900 via one or more of its ports regardless of the RADIUS server, invoke the command:

**port PORTS-GROUP mode force-unauth**

where,

**PORTS-GROUP**: Group of ports.

**force-unauth**: Prevent access via the ports regardless of the RADIUS server.

## Disabling the IEEE 802.1x Protocol on Ports

To *disable* the IEEE 802.1x protocol on one or more OS900 ports, invoke the command:

**port PORTS-GROUP mode disable**

where,

**PORTS-GROUP**: Group of ports.

**disable**: Disable the IEEE 802.1x protocol on the ports.

## Maximum Number of Request Retransmissions

To change the maximum number of times a client request will be retransmitted to the RADIUS server, invoke the command:

**`port PORTS-GROUP max-req <0-10>`**

where,

**`PORTS-GROUP`**: Group of ports.

**`<0-10>`**: Maximum number of retransmissions.

(To revert to the default maximum number of request retransmissions (2), invoke the command:

**`no port PORTS-GROUP max-req`**.)

## Multiple Client MACs per Port

To allow/prevent more than one client MAC per port, invoke the command:

**`port PORTS-GROUP multi-hosts (enable|disable)`**

where,

**`PORTS-GROUP`**: Group of ports.

**`enable`**: Allow multiple client MACs per port.

**`disable`**: Prevent multiple client MACs per port, i.e., allow only the authorized client.

(To revert to the default (disable), invoke the command:

**`no port PORTS-GROUP multi-hosts`**.)

## Server Timeout

To change the time the OS900 is to wait for a reply from the RADIUS server before retransmitting a packet, invoke the command:

**`port PORTS-GROUP server-timeout <1-65535>`**

where,

**`PORTS-GROUP`**: Group of ports.

**`server-timeout`**: Wait for a reply from server before retransmiting a packet to it.

**`<1-65535>`**: Wait time (in seconds).

(To revert to the default wait time (30 seconds), invoke the command:

**`no port PORTS-GROUP server-timeout`**.)

## Wait Time

To change the time the OS900 is to wait (before transmitting a client request to the RADIUS server) following a failed authentication exchange with the client, invoke the command:

**`port PORTS-GROUP quiet-period <1-65535>`**

where,

**`PORTS-GROUP`**: Group of ports.

**`quiet-period`**: Wait following a failed authentication exchange with client.

**`<1-65535>`**: Wait time (in seconds).

(To revert to the default wait time (60 seconds), invoke the command:

**`no port PORTS-GROUP quiet-period`**.)

## Periodic Reauthentication

To initiate reauthentication periodically, invoke the command:

**`port PORTS-GROUP periodic-reauth enable [<1-65535>]`**

where,

**`PORTS-GROUP`**: Group of ports.

**`periodic-reauth`**: Initiate reauthentication periodically.

**`enable`**: Enable periodic reauthentication (Default period: 3600 seconds).

**<1-65535>**: Reauthentication period (in seconds).

(To revert to the default (disable), i.e., to disable periodic reauthentication, invoke the command:
**no port PORTS-GROUP periodic-reauth**.)

# Viewing

## IEEE 802.1X Protocol Operative Status

To view the IEEE 802.1X Protocol operative status of the OS900:

1. Enter **enable** mode or **dot1x** mode.
2. Invoke the command:
   **show dot1x**

Example

```
OS910(config-dot1x)# show dot1x
Dot1x Global Mode: enabled
OS910(config-dot1x)#
```

The example above shows that the IEEE 802.1X protocol has been '`enabled`' for the OS900 using the command **enable**.

## Port Status and Configuration

To view the IEEE 802.1X Protocol operative status and configuration of the OS900 ports:

1. Enter **enable** mode or **dot1x** mode.
2. Invoke the command:
   **show dot1x port PORTS-GROUP**
   where,
   **PORTS-GROUP**: Group of ports whose IEEE 802.1X protocol status and configuration are to be viewed.

Example

```
OS910(config-dot1x)# show dot1x port 2
Dot1x Global Mode: enabled
  Dot1x Port 2    :
    Status:            unauthorized     Mode:            auto
    Max req:           2                Multi hosts:     enabled
    Server timeout:   30 seconds        Quiet period:   60 seconds
    Periodic reauth:   enabled          Reauth period: 3600 seconds
OS910(config-dot1x)#
```

In the example above:

'`Dot1x Global Mode`' indicates whether the IEEE 802.1X protocol is '`enabled`' or '`disabled`'.

'`Status`' indicates whether the RADIUS server has '`authorized`' or '`unauthorized`' access.

'`Mode`' indicates whether the OS900 port is set to the mode:

- '`auto`': Allow RADIUS server to perform authentication and to permit or deny access.
- '`force-auth`': Enable access regardless of the RADIUS server.
- '`force-unauth`': Disable access regardless of the RADIUS server.
- '`disable`': Disable the IEEE 802.1x protocol.

'`Max req `' indicates the maximum number of times a request will be retransmitted to the RADIUS server.

'`Multi hosts`' indicates whether more than one client MAC per port is '`enabled`' or '`disabled`'.

'`Server timeout`' indicates the time the OS900 is to wait for a reply from the RADIUS server before retransmitting a packet.

'`Quiet period`' indicates the time the OS900 is to wait (before transmitting a client request to the RADIUS server) following a failed authentication exchange with the client.

'`Periodic reauth`' indicates whether periodic reauthentication is '`enabled`' or '`disabled`'.

'`Reauth period`' indicates the reauthentication period.

# Chapter 25: IP SLA

## General

IP SLA is a service assurance tool that enables service providers to monitor and measure the performance of Layer 3 IP VPN routing networks. It is a real-time application using the ICMP protocol and is based on RFC 2925. Its OAM hardware acceleration engine enables it to provide performance measurement based on the ITU-T SG 13 Y.1731 standard with nanosecond accuracy.

IP SLA tests are run between two OS900s.

Up to four tests[65] can be run concurrently. However, over a 100 tests can be run using the scheduler function described in ***Chapter 27:*** *Scheduler*, page *499*. Using this function, the tests (each time-limited) are preset to be run in succession. As soon as any of four tests is completed, the next test is automatically run.

The tests can be run at Layer 2 (Hardware-accelerated) or Layer 3 (CPU-based).

## Purposes

To:

- Test connectivity and performance between the OS900 and other devices over IP-routing service networks.
- Determine the Round-Trip Delay (RTD), jitter, and packet loss when communicating with a target device
- Collect IP SLA probe (test) history
- Collect statistical data for predicting and remodeling network operation
- Generate SNMP traps and Alerts

## Modes

IP SLA testing can be run in *CPU-based* or *hardware-accelerated* mode. *Table 21*, below, compares the two modes.

**Table 21: CPU-based *versus* Hardware-accelerated IP SLA Testing**

| CPU-based | Hardware-accelerated |
|---|---|
| *Requires* CPU processing | *Does not require* CPU processing (thereby freeing the CPU for other tasks) |
| Tests run at speeds of up to 50 pps | Tests are run at wirespeed |
| Measurements are performed with *millisecond* accuracy | Measurements are performed with *nanosecond* accuracy |
| Packet lengths of only up to *1500* bytes are supported | Packet lengths of up to *9216* bytes are supported |

## Requirements

To run IP SLA tests between two OS900s, two *Inband VLAN interfaces*, one on each OS900, must be configured for running the tests between them. (The procedure for configuring Inband VLAN

[65] The tests can be RFC 2544, IP SLA, Y.7131 Delay Measurement, and Y.7131 Loopback.

interfaces is described in ***Chapter 7:*** *Interfaces*, page *177*.) These *Inband VLAN interfaces* cannot participate in *hardware*-controlled routing!

To run *hardware-accelerated* IP SLA tests:

1. Both OS900s must have FPGA. (An OS900 has an FPGA if it is possible to invoke the command **`show fpga version`** from **`enable`** mode).
2. The Inband VLAN interfaces between which the *hardware-accelerated* test is to be run must both be configured to *hardware-accelerated* IP SLA mode by invoking the command **`ip sla`** in the modes of the Inband VLAN interfaces.

# Configuring and Running a Probe

The minimum steps for configuring and running an IP SLA probe are:

– For *hardware-accelerated* IP SLA testing, invoking the command **`ip sla`** in the modes of the Inband VLAN interfaces between which the *hardware-accelerated* test is to be run
– Creating a Probe with default parameter values
– Defining the Destination IP Address for the Probe
– Running the Probe

The procedures for changing the default parameter values are given in the section *Optional Configuration Parameters for Probes*, page *475*.

## Creating a Probe (or Entering its Mode)

To create a probe with default parameter values and/or to enter its mode:

1. Enter **`configure terminal`** mode.
2. Invoke either of the following commands:

   **`ip sla monitor OWNER [NAME [TARGET]]`**

   **`ip sla monitor OWNER [NAME [enable]] [slow]`**

   where,

   **`OWNER`**: Owner name (e.g., Jojo)

   **`[NAME]`**: Probe/test name (e.g., Probe-1). Default: **`*`**

   **`[TARGET]`**: Target (destination) address or hostname

   **`[enable]`**: Run the probe (enable transmission)

   **`[slow]`**: *CPU-based* performance measurement. (This argument exists only for OS900s having an FPGA.)
   Default: *Hardware-accelerated* performance measurement. (*Hardware-accelerated* performance measurement provides for presenting time parameters with extremely higher accuracy, i.e., in nanoseconds!)
   For OS900s having an FPGA, *CPU-based* performance measurement is optional. For OS900s that do not have an FPGA, *CPU-based* performance measurement is enforced.
   In *hardware-accelerated* performance measurement, the maximum length allowed for packets is 9216 bytes. In *CPU-based* performance measurement, the maximum length allowed is 1500 bytes.

Several probe names can be defined per owner name.

Example

```
OS912C(config)# ip sla monitor OWNER_1 Probe-1
OS912C(config-ip-sla)#
```

## Defining a Destination IP Address for a Probe

To define a destination IP address for a probe

1. Enter the mode of the probe.
2. Invoke the command:
   **dest-ip TARGET**
   where,
   **TARGET**: Target IP address or hostname.

Example

```
OS912C(config-ip-sla)# dest-ip 10.0.0.2
OS912C(config-ip-sla)#
```

## Running a Probe

A probe can be run using either Method 1 or 2 below.

### Method 1

1. Enter **configure terminal** mode.
2. Invoke the command
   **ip sla monitor OWNER [NAME [enable]] [slow]**
   where,
   **OWNER**: Owner name (e.g., Jojo)
   **[NAME]**: Probe/test name (e.g., Probe-1). Default: *
   **[enable]**: Run the probe (enable transmission)
   **[slow]**: *CPU-based* performance measurement. (This argument exists only for OS900s having an FPGA.)
   Default: *Hardware-accelerated* performance measurement. (*Hardware-accelerated* performance measurement provides for presenting time parameters with extremely higher accuracy, i.e., in nanoseconds!)
   For OS900s having an FPGA, *CPU-based* performance measurement is optional. For OS900s that do not have an FPGA, *CPU-based* performance measurement is enforced.
   In *hardware-accelerated* performance measurement, the maximum length allowed for packets is 9216 bytes. In *CPU-based* performance measurement, the maximum length allowed is 1500 bytes.

Example

```
OS912C(config)# ip sla monitor OWNER_1 Probe-1 enable
OS912C(config)#
```

### Method 2

1. Enter the mode of the probe
2. Invoke the command:
   **enable [slow]**
   where,
   **[slow]**: *CPU-based* performance measurement. (This argument exists only for OS900s having an FPGA.)
   Default: *Hardware-accelerated* performance measurement. (*Hardware-accelerated* performance measurement provides for presenting time parameters with extremely higher accuracy, i.e., in nanoseconds!)
   For OS900s having an FPGA, *CPU-based* performance measurement is optional. For OS900s that do not have an FPGA, *CPU-based* performance measurement is enforced.
   In *hardware-accelerated* performance measurement, the maximum length allowed for packets is 9216 bytes. In *CPU-based* performance measurement, the maximum length allowed is 1500 bytes.

Example

```
OS912C(config-ip-sla)# enable
OS912C(config-ip-sla)#
```

### Example

The following example demonstrates configuration and running of a probe.

```
OS912C# show running-config
Building configuration...
Current configuration:
! version 2_1_4
!
interface vlan vif10
 tag 10
 ip 10.0.0.1/24
 ports 1-2
 ip sla
!
OS912C# configure terminal
OS912C(config)# ip sla monitor Jojo MRV1
OS912C(config-ip-sla)# dest-ip 10.0.0.2
OS912C(config-ip-sla)# enable
```

# Stopping a Probe

A probe can be stopped before test completion using Method 1 or 2 below.

**Method 1**

1. Enter **configure terminal** mode.
2. Invoke the command

   **no ip sla monitor OWNER NAME enable**

   where,

   **OWNER**: Owner name (e.g., Jojo)

   **[NAME]**: Probe/test name (e.g., Probe-1). Default: *

Example

```
OS912C(config)# no ip sla monitor OWNER_1 Probe-1 enable
OS912C(config)#
```

**Method 2**

To stop a probe before test completion:

1. Enter the mode of the probe
2. Invoke the command

   **no enable**

Example

```
OS912C(config-ip-sla)# no enable
OS912C(config-ip-sla)#
```

# Viewing

## Configurations and Results of the Probes

To view the configurations and results of all the probes:

1. Enter **enable** mode.
2. Invoke the command:

   **show ip sla**

## Result of a Probe

To view the last result of a probe:

1. Enter the mode of the probe.
2. Invoke the command:

   **`show ip sla`**

Example

```
OS900# show ip sla
----------- type:monitor owner:'1' testname:'1' stopped
 burst-number:      5       burst-interval: 10 sec
 length:           88       packets:        100
 ttl:             128       timeout:        200 ms
 history-size:     10       interval:       1000 us
 dest-ip:      100.1.1.2
 zero trap mask
 Resolved target: 100.1.1.2
 Started at Tue Jun 30 20:16:56 2009
 5 lines in history table.
 Priority: 0, Tos: 0
 100 packets transmitted; 100 packets received, 0.00% packet loss
 Round-trip min/avg/max: 14.672/14.720/14.800 us
 Jitter min/avg/max: 0.000/0.000/-0.080 us
 Last good probe: Tue Jun 30 20:17:46 2009
OS900#
```

## History of a Probe

To view the history of a probe, Method 1 or 2 below can be used.

### Method 1

1. Enter **`enable`** mode.
2. Invoke the command:

   **`show ip sla OWNER NAME history`**

   where,

   **`OWNER`**: Owner name (e.g., Jojo)

   **`NAME`**: Probe/test name (e.g., Probe-1).

Example

```
OS906C(config-ip-sla)# show ip sla 1 1 history
----- Resolved target: 10.10.10.4-----
 Started at Tue Jun 30 16:47:27 2009
 Priority: 6, Tos: 5
 10 packets transmitted; 10 packets received, 0.00% packet loss
 Round-trip min/avg/max: 14.576/14.600/14.656 us
 Jitter min/avg/max: 0.000/-0.002/-0.048 us
OS906C(config-ip-sla)#
```

Jitter, RTD, and packet loss values, in addition to bandwidth, serve to determine whether the network in its present configuration can provide the requisite level of service essential for time-sensitive applications such as VoIP and video streaming. For VoIP, a delay (time it takes for an ICMP request to reach its destination) of up to 150 ms is usually acceptable.

Jitter is defined as the **current RTD – previous RTD**. Accordingly, jitter may be positive or negative. Three jitter values are recorded by the OS900:

Jitter min – The minimum jitter recorded.

Jitter avg – The average of the jitters recorded.

Jitter max – The maximum jitter recorded.

RTD is defined as the time between sending an ICMP request and receiving the corresponding response.

Packet loss ratio as a percentage (i.e., [packets sent – packets received]/[packets sent] x 100).

**Method 2**

1. Enter the mode of the probe.
2. Invoke the command:
   **`show ip sla history`**

Example

```
OS906C(config-ip-sla)# show ip sla history
----- Resolved target: 10.10.10.4-----
 Started at Tue Jun 30 16:47:27 2009
 Priority: 6, Tos: 5
 10 packets transmitted; 10 packets received, 0.00% packet loss
 Round-trip min/avg/max: 14.576/14.600/14.656 us
 Jitter min/avg/max: 0.000/-0.002/-0.048 us
OS906C(config-ip-sla)#
```

## Brief Information on all Probes

To view the name, owner name, and operation status (running or stopped) of all configured probes:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show ip sla brief`**

Example

```
OS912C# show ip sla brief
ip sla monitor OWNER_1    Probe-1    running
ip sla monitor OWNER_1    Probe-2    stopped
ip sla monitor OWNER_2    Probe-A    stopped
3 entries, 1 running
OS912C#
```

## Detailed Configuration Information on a Probe

To view detailed run-time configuration information on a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **`show`**

Example 1

```
OS900(config-ip-sla)# show



 ----------- type:monitor owner:'OWNER_1' testname:'Probe-1' stopped
burst-number:      1       burst-interval: 60 sec
 length:           88       packets:        10
 ttl:             128       timeout:        200 ms
 history-size:     10       interval:       100000 us
 tos:             5
 priority:        6
 dest-ip:      10.10.10.4
 zero trap mask
 Resolved target: 10.10.10.4
 Started at Tue Jun 30 16:47:27 2009
 1 lines in history table.
 Priority: 6, Tos: 5
 10 packets transmitted; 10 packets received, 0.00% packet loss
 Round-trip min/avg/max: 14.576/14.600/14.656 us
 Jitter min/avg/max: 0.000/-0.002/-0.048 us
 Last good probe: Tue Jun 30 16:48:27 2009
OS900(config-ip-sla)#
```

## Configuration Information on Probes

To view run-time SLA Configuration information for probes, Method 1 or 2 can be used.

**Method 1**

1. Enter **enable** mode.
2. Invoke the command:
   **show ip sla configuration**

Example

```
OS912C# show ip sla configuration
!
! Service Level Agreement configuration
!
ip sla monitor OWNER_1 Probe-1
 dest-ip  10.90.136.1
 trap all
ip sla monitor OWNER_1 Probe-2
 dest-ip  localhost
ip sla monitor OWNER_2 Probe-A
 dest-ip  localhost
OS912C#
```

**Method 2**

1. Enter the mode of a probe.
2. Invoke the command:
   **show configuration**

Example 1

```
OS912C(config-ip-sla)# show configuration
! Service Level Agreement configuration
!
ip sla monitor OWNER_1 Probe-1
 dest-ip  10.90.136.1
 trap all
ip sla monitor OWNER_1 Probe-2
 dest-ip  localhost
ip sla monitor OWNER_2 Probe-A
 dest-ip  localhost
OS912C(config-ip-sla)#
```

## Default Parameter Values for a Probe

To display the default values used for the parameters of a probe:

1. Enter **enable** mode.
2. Invoke the command:
   **show ip sla defaults**

Example 1

```
OS912C# show ip sla defaults
Parameter                       Default values
----------------------------------------------------------------
  burst-interval                60 sec
  burst-number                  1
  history-size                  5 entries
  interval                      100000 usec
  length                        68 bytes (without CRC)
  packets                       3
  priority                      0
  timeout                       200 msec
  tos                           0
  ttl                           128
OS912C#
```

The parameters in the above example mean the following:

| | |
|---|---|
| `burst-interval`: | Time interval between every two bursts |
| `burst-number`: | Number of packet transmission bursts |
| `history-size`: | Number of most recent history entries to be stored |
| `interval`: | Time interval between every two packets in a burst |
| `length`: | PDU length that will help diagnose faults sensitive to this length |
| `packets`: | Number of packets to be sent during each burst interval |
| `priority`: | Layer 2 PDU priority |
| `timeout`: | Maximum time the IP SLA mechanism is to wait for a response to a request PDU |
| `tos`: | IP ToS field and value: |
| `ttl`: | Time-to-live for linktrace packets |

## Commands in a Probe Mode

To display the list of commands in the mode:

1. Enter the mode of a probe.
2. Press ?.

Example

```
OS912C(config-ip-sla)# ?
  burst-interval  Time interval between bursts (sec)
  burst-number    Number of times to perform a burst
  clear           Clear
  default         Reset all parameters
  description     Description for current entry
  dest-ip         Set target address
  enable          Enable transmission
  history-size    Number of entries in history table
  interval        Time interval between packets (usec)
  length          Packet length including VLAN-id and CRC
  no              Negate a command or set its defaults
  packets         Number of packets to send in one burst
  pattern         Pattern (DataFill) of DataTLV
  priority        VLAN tag P-bits (PCP)
  show            show current entry
  timeout         Time to wait for test completion (msec).
  tos             IP Type-Of-Service field of sent packets
  trap            Probe notifications control
  ttl             Time-To-Live field of sent packets
```

```
OS912C(config-ip-sla)#
```

# Optional Configuration Parameters for Probes

This section provides procedures for changing parameter values of a probe.

To change a parameter value, first enter the mode of a probe.

## Service Level (SL)

To set the SL for a probe, invoke the command:

**sl <1-8>**

where,

**<1-8>**: SL to be selected from the range 1 to 8

To reset the SL for a probe to the default value (1), invoke the command:

**no sl**

## Description for a Probe

### Adding/Replacing

To add/replace a textual description of a probe:

1. Enter the mode of the probe.
2. Invoke the command:

   **description ..**

   where,

   **description**: Textual description.

   **..**: Textual description.

Example

```
OS912C(config-ip-sla)# description Marketing Department
OS912C(config-ip-sla)#
```

### Deleting

To delete the textual description of a probe:

1. Enter the mode of the probe.
2. Invoke the command:

   **no description**

Example

```
OS912C(config-ip-sla)# no description
OS912C(config-ip-sla)#
```

## Number of Bursts

### Custom

To set the number of packet transmission bursts for a probe

1. Enter the mode of the probe.
2. Invoke the command:

   **burst-number <1-255>|unlimited**

   where,

   **<1-255>**: Number of bursts to be selected from the range 1-255. Default: 1

   **unlimited**: Continuous transmission

Example

```
OS912C(config-ip-sla)# burst-number 13
OS912C(config-ip-sla)#
```

**Default**

To reset the burst number to the default value (**1**), invoke the command:

1. Enter the mode of the probe.
2. Invoke the command:
   **no burst-number**

Example

```
OS912C(config-ip-sla)# no burst-number
OS912C(config-ip-sla)#
```

## Burst Interval

**Custom**

To set the time interval between every two bursts for a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **burst-interval <1-86400>**

   where,

   **<1-86400>**: Burst interval (in seconds) to be selected from the range 1 to 86400. Default **60**.

Example

```
OS912C(config-ip-sla)# burst-interval 75
OS912C(config-ip-sla)#
```

**Default**

To reset the burst interval to the default value (**60**):

1. Enter the mode of the probe.
2. Invoke the command:
   **no burst-interval**

Example

```
OS912C(config-ip-sla)# no burst-interval
OS912C(config-ip-sla)#
```

| | Notes<br>Note that the Time Interval can influence the Burst Interval and vice versa. |
|---|---|

## Number of History Entries

**Custom**

To limit the number of most recent history entries to be stored for a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **history-size <2-65535>**

   where,

   **<2-65535>**: Maximum number of history entries to be recorded from the range 2 to 65535. Default: **5**

Example

```
OS912C(config-ip-sla)# history-size 12
OS912C(config-ip-sla)#
```

### Default

To reset the number of history entries to the default value (`5`):

1. Enter the mode of the probe.
2. Invoke the command:
   **`no history-size`**

Example

```
OS912C(config-ip-sla)# no history-size
OS912C(config-ip-sla)#
```

## Time Interval

### Custom

To set the time interval between every two packets in a burst for a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **`interval <1-1000000>`**

   where,

   **`<1-1000000>`**: Time interval *in microseconds* to be selected from the range 1 to 1,000,000. Default: **`100000`**

Example

```
OS912C(config-ip-sla)# interval 200000
OS912C(config-ip-sla)#
```

### Default

To reset the time interval to the default value (`100000`):

1. Enter the mode of the probe.
2. Invoke the command:
   **`no interval`**

Example

```
OS912C(config-ip-sla)# no interval
OS912C(config-ip-sla)#
```

**Notes**

Note that the Burst Interval can influence the Time Interval and vice versa.

## PDU Length

### Custom

To set the PDU length (includes L2VPT [802.1p] field bits and CRC) for a probe that will help diagnose faults sensitive to this length:

1. Enter the mode of the probe.
2. Invoke the command:
   **`length <64-9216>`**

   where,

   **`<64-9216>`**: PDU length (in octets) to be selected from the range 64 to 9216. In the *CPU-based* mode, the minimum length selectable is **`88`**. Default: **`68`**.

Example

```
OS912C(config-ip-sla)# length 137
OS912C(config-ip-sla)#
```

### Default

To reset the PDU length to the default value (**68**):

1. Enter the mode of the probe.
2. Invoke the command:
   **no length**

Example

```
OS912C(config-ip-sla)# no length
OS912C(config-ip-sla)#
```

## Number of Packets

### Custom

To set the number of packets to be sent during each burst interval for a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **packets <1-1000000>**

   where,

   **<1-1000000>**: Number of packets to be sent to be selected from the range 1 to 1,000,000. Default: **3**.

Example

```
OS912C(config-ip-sla)# packets 18
OS912C(config-ip-sla)#
```

### Default

To reset the number of packets to be sent to the default value (**3**):

1. Enter the mode of the probe.
2. Invoke the command:
   **no packets**

Example

```
OS912C(config-ip-sla)# no packets
OS912C(config-ip-sla)#
```

## Data Pattern

### Adding

To add a data pattern (inside a PDU) that will help to diagnose faults sensitive to incompleteness of data in a packet for a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **pattern HEXLINE**

   where,

   **HEXLINE**: Pattern (dataFill) of DataTLV using hexadecimal digits, e.g., **0123fa9c**. The number of characters must be an integral multiple of 8.

   If the PDU length is greater than the pattern size, the pattern is repeated until the total length is equal to the PDU.

   If the PDU length is less than the pattern size, the pattern is truncated to the PDU length.

Example

```
OS912C(config-ip-sla)# pattern 0123fa9c
OS912C(config-ip-sla)#
```

#### Deleting

To delete the data pattern:

1. Enter the mode of the probe.
2. Invoke the command:
   **`no pattern`**

Example

```
OS912C(config-ip-sla)# no pattern
OS912C(config-ip-sla)#
```

### Layer 2 PDU Priority

#### Custom

To set the L2VPT (802.1p) field bits for and accompanying a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **`priority [<0-7>]`**

   where,

   **`[<0-7>]`**: Layer 2 PDU priority to be selected from the range 0 (lowest priority) to 7 (highest priority). Default: `0`.

Example

```
OS912C(config-ip-sla)# priority 6
OS912C(config-ip-sla)#
```

#### Default

To reset the Layer 2 PDU priority to the default value (`0`):

1. Enter the mode of the probe.
2. Invoke the command:
   **`no priority`**

Example

```
OS912C(config-ip-sla)# no priority
OS912C(config-ip-sla)#
```

### Timeout

#### Custom

To set the maximum time the IP SLA mechanism is to wait for a response to its probe request PDU:

1. Enter the mode of the probe.
2. Invoke the command:
   **`timeout <1-60000>`**

   where,

   **`<1-60000>`**: Wait time (in milliseconds) from the range 0 to 60000. Default: **`200`**.

Example

```
OS912C(config-ip-sla)# timeout 450
OS912C(config-ip-sla)#
```

### Default

To reset the wait time to the default value (**200**):

1. Enter the mode of the probe.
2. Invoke the command:
   **no timeout**

Example

```
OS912C(config-ip-sla)# no timeout
OS912C(config-ip-sla)#
```

## Time-To-Live

### Custom

To set the time-to-live for packets:

1. Enter the mode of the probe.
2. Invoke the command:
   **ttl <1-255>**

   where,
   **<1-255>**: Time-to-live for linktrace packets from the range 1 to 255. Default: **128**.

Example

```
OS912C(config-ip-sla)# ttl 97
OS912C(config-ip-sla)#
```

### Default

To reset the time-to-live to the default value (**128**):

1. Enter the mode of the probe.
2. Invoke the command:
   **no ttl**

Example

```
OS912C(config-ip-sla)# no ttl
OS912C(config-ip-sla)#
```

## DiffServ ToS (DSCP)

### Custom

To change the value of the IP ToS field that accompanies the probe packet:

1. Enter the mode of the probe.
2. Invoke the command:
   **tos <0-255>**

   where,
   **<0-255>**: ToS value from the range 0 to 255. Default: **0**.

Example

```
OS912C(config-ip-sla)# tos 78
OS912C(config-ip-sla)#
```

### Default

To set the value of the IP ToS field that accompanies the probe packet to the default (**0**):

1. Enter the mode of the probe.
2. Invoke the command:
   **no tos**

Example

```
OS912C(config-ip-sla)# no tos
OS912C(config-ip-sla)#
```

# Resetting all Parameters of a Probe

To reset all parameters of a probe to their default values:

1. Enter the mode of the probe.
2. Invoke the command:
   **`default`**

Example

```
OS912C(config-ip-sla)# default
OS912C(config-ip-sla)#
```

# Clearing Statistics on a Probe

To clear all statistics on a probe:

1. Enter the mode of the probe.
2. Invoke the command:
   **`clear statistics`**

Example

```
OS912C(config-ip-sla)# clear statistics
OS912C(config-ip-sla)#
```

# Traps for Probes

An SNMP trap is sent as defined in PING.txt of RFC 2925.

## Enabling

To enable the OS900 agent to send SNMP traps for probes:

1. Enter the mode of the probe.
2. Invoke the command:
   **`trap (all|testCompletion|pathChange)`**

   where,

   **`all`**: Generate test completion and path notifications.
   **`testCompletion`**: Generate test completion notification.
   **`pathChange`**: Generate path change notification.

Example

```
OS912C(config-ip-sla)# trap testCompletion
OS912C(config-ip-sla)#
```

## Disabling

To disable the OS900 agent from sending SNMP traps for probes:

1. Enter the mode of the probe.
2. Invoke the command:
   **`no trap (all|testCompletion|pathChange)`**

   where,

   **`all`**: Generate test completion and path notifications.
   **`testCompletion`**: Generate test completion notification.
   **`pathChange`**: Generate path change notification.

Example

```
OS912C(config-ip-sla)# no trap testCompletion
OS912C(config-ip-sla)#
```

## Probe Failures

To enable the OS900 agent to send SNMP traps for probe failures:

1. Enter the mode of the probe.
2. Invoke either of the following equivalent commands:

   **trap probeFailure filter <0-15>**

   **trap filter probeFailure <0-15>**

   where,

   **<0-15>**: Number of events before sending a notification.

Example

```
OS900(config-ip-sla)# trap probeFailure filter 3
OS900(config-ip-sla)#
```

## Test Failures

To enable the OS900 agent to send SNMP traps for test failures:

1. Enter the mode of the probe.
2. Invoke either of the following equivalent commands:

   **trap testFailure filter <0-15>**

   **trap filter testFailure <0-15>**

   where,

   **<0-15>**: Number of events before sending a notification.

Example

```
OS900(config-ip-sla)# trap testFailure filter 4
OS900(config-ip-sla)#
```

# **Chapter 26:** RFC 2544 Testing

## General

The OS900 has the capability of performing *hardware-accelerated* (wire-speed*)* RFC 2544 testing from its internal traffic generator[66] and analyzing the echoed traffic. This enables a provider to run RFC 2544 tests on an Ethernet connection from a management station easily and at anytime instead of sending a technician to the customer sites to perform these tests.

An RFC 2544 test can be run through either of the following services:

- Ethernet Private Line (EPL)
- Ethernet Virtual Private Line (EVPL)

RFC 2544 tests can be run between two OS900s or between an OS900 and another switch provided the latter can operate with Layer 2 and Layer 3 packets and with speeds of up to at least 1 Gbps so as not to lose traffic data.

Up to four tests[67] can be run concurrently.

However, over a 100 tests can be preset and run either by the internal mechanism of the OS900 or using the scheduler function described in ***Chapter 27:*** *Scheduler*, page *499*. Using this function, the tests (each time-limited) are preset to be run in succession. As soon as any of four tests is completed, the next test is automatically run.

The internal mechanism schedules running of the tests in round-robin fashion. That is, as soon as a test runs one burst of packets[68] it is sent to the end of the wait queue if it is scheduled to run more than once. Here the test waits until the end of its burst interval and until it reaches the front of the queue. As soon as one of the four tests running concurrently is completed, the test is run again.

The tests can be run at Layer 2 or Layer 3.

The OS900's SNMP agent supports osRfc2544.mib so that RFC 2544 tests can also be run from an SNMP Manager. For details, refer to the *MegaVision User Manual*.

## Requirement

Both OS900s must have FPGA. (An OS900 has an FPGA if it is possible to invoke the command **`show fpga version`** from **`enable`** mode).

## Types of Test

At Layer 2 and 3, the following tests can be run:

- ***Default***. In this test, the set rate (using the command **`rate RATELIMIT`** – described below) is fixed throughout the test. The test is run once without interruption. It is the default test.
- ***Throughput***. This test can be used to determine whether there is packet throughput loss. In this test, the set rate is reduced if there is packet loss. Following is a description of the mechanism that runs this type of test: If during the test packet loss exceeds the maximum permitted % loss acceptable (described in the section *Percentage Loss*, page *491*), the test is rerun at 50% of the set rate. The rate will be reduced by 50% of the *current* rate each time there is packet loss. If for a reduced rate packet loss stops, the rate will be increased

[66] Creates and transmits a stream of Layer 2 frames.

[67] The tests can be RFC 2544, IP SLA, Y.7131 Delay Measurement, and Y.7131 Loopback.

[68] The number of packets to be sent in a burst interval can be set using the command given in the section Number of Packets*, page 492*.

by 50% of the *current* rate and the test rerun. If there is no packet loss, the rate will be increased by an additional 50% of the *previous* rate increase. This will be continued until the rate increase is ≤ 1 Mbps.
The following example is used to demonstrate how the throughput mechanism works. The set rate selected is 64 Mbps.

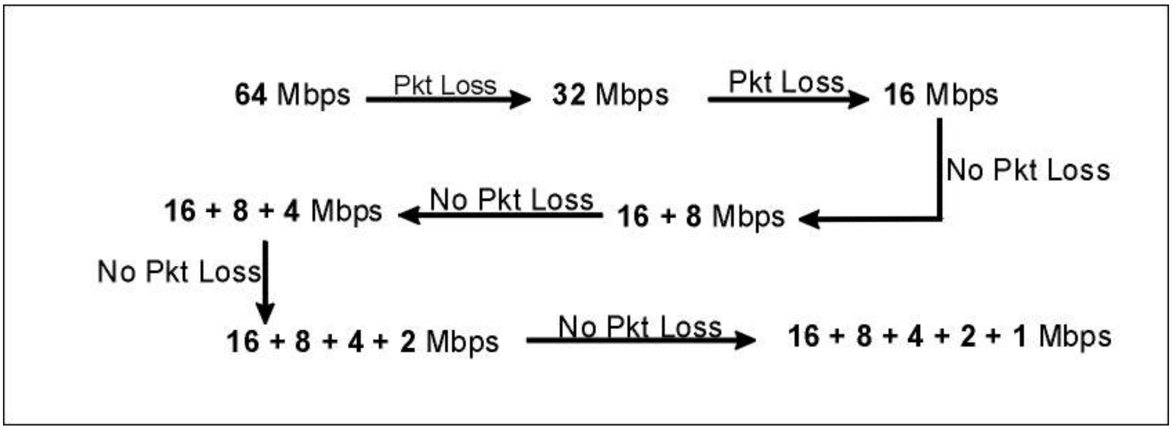



**Figure 43: Demonstration of how the Throughput Mechanism Works**

In the above diagram, the final rate at which the test will be run is:
16 + 8 + 4 + 2 +1 (= 31) Mbps.
Notice that the mechanism selects a rate that is at most 1 Mbps short of the highest possible rate for which there is no packet loss.

# Layer 2 Testing

## Setup

To run Layer 2 RFC 2544 tests between two OS900s (responder and initiator), set them up as follows:

<u>Responder OS900 (at which frames are to be received)</u>

1. Configure an inband VLAN interface via which test frames are to be transmitted as described in the section *Configuring*, page *181*.
2. Specify the MAC address of the Responder OS900 inband VLAN interface by invoking the command:
   **`rfc2544 mac-to-responder HEXLINE`**
   where,
   **`HEXLINE`**: MAC address in hex format. Make sure that the MAC address is in the range **`xx.xx.xx.YY.xx.xx`** where, **`xx`** designates the hex pair in the MAC address of the inband VLAN interface and **`YY`** is a hex pair in the range **`01`** to **`FE`** (e.g., **`00:0F:BD:F3:5E:84`**).

<u>Initiator OS900 (from which frames are to be transmitted)</u>

1. Configure an inband VLAN interface via which test frames are to be transmitted as described in the section *Configuring*, page *181*.
2. Specify the MAC address of the Initiator OS900 inband VLAN interface by invoking the command:
   **`rfc2544 mac-to-responder HEXLINE`**
   where,
   **`HEXLINE`**: MAC address in hex format. Make sure that the MAC address is in the range **`xx.xx.xx.YY.xx.xx`** where, **`xx`** designates the hex pair in the MAC address of the inband VLAN interface and **`YY`** is a hex pair in the range **`01`** to **`FE`** (e.g., **`00:0F:BD:F3:5E:84`**).
3. Enter **`configure terminal`** mode.
4. Create a test (enter the mode of a test) by invoking the command:

**rfc2544 tester OWNER NAME**

where,

**OWNER**: Owner name (e.g., Jojo)

**[NAME]**: Test name (e.g., Test-1). Default: *

(To delete the test, enter **configure terminal** mode and invoke the command **no rfc2544 tester OWNER [NAME]**.)

5. If the type of test is not selected, the ***Default*** test is run. Select the type of test by invoking the command:

   **test default|throughput**

   where,

   **default**: Default test.

   **throughput**: Throughput test.

6. Specify the tag of the inband VLAN interface by invoking the command:

   **vlan <1-4093>**

   where,

   **<1-4093>**: VLAN tag that is the same as that specified in step *1*, page *482*, above

   (To delete the VLAN, invoke the command **no vlan**.)

7. Specify Delay Measurement (Layer 2 testing) by invoking the command:

   **type delay-measure**

8. Specify the MAC address of the Responder OS900 inband VLAN interface by invoking the command:

   **dest-mac TARGET**

   where,

   **TARGET**: MAC address as specified in step *2*, page *484*, above for the Responder OS900.

9. In the event that the MAC address of the Responder OS900 is not learnt, the test can run if a physical port via which the datastream is to be transmitted is specified. If the MAC address of the Responder OS900 is learnt, the user specified port is ignored.

   To specify the physical port, invoke the command:

   **port PORT**

   where,

   **PORT**: Number of the port.

10. The default rate of the test frames is 64 Kbps. To specify any rate, invoke the command:

    **rate RATELIMIT**

    where,

    **RATELIMIT**: Rate of the test frames in bits per second.
    Range is 64 Kbps to 1 Gbps.
    In *default* test the rate of the transmitted test string is fixed.
    In *throughput* test the rate of the sent test string is the maximum.

Example

**Initiator OS900**

```
---------
interface vlan vif4
 tag 10
 ports 1,3
 rfc2544 mac-to-responder 00:0F:BD:01:7A:66
!
rfc2544 tester Jojo Test-1
 vlan 10
 type delay-measure
 dest-mac 00:0F:BD:01:6E:54
```

```
 rate 1g
 packets 10  (This setting is optional !)
 port 1
```

**Responder OS900**

```
---------
interface vlan vif10
 tag 10
 ports 1,3
 rfc2544 mac-to-responder 00:0F:BD:01:6E:54
```

## Running a Test

To run a test that has been set up (as described in the section *Setup*, page *484*), at the Initiator OS900:

1. Enter the mode of the test (as described in Step *4*, page *484*)
2. Invoke the command:
   **`enable`**

## Viewing Test Results

To view the test results:

1. Enter the mode of the test (as described in Step *4*, page *484*)
2. Invoke the command:
   **`show`**

Example

```
OS900(config-rfc2544)# show

 ----------- type:tester owner:'Jojo' testname:'Test-1' stopped
 vlan:             10       type:           delay-measure
 length:           68       packets:        10
 ttl:             128       timeout:        200 ms
 history-size:     10       rate:           1g
 port:              1       dest-mac:       00:0F:BD:01:6E:54
 Target mac: 00:0F:BD:01:6E:54
  Started at Wed Jul 14 17:12:36 2010
 1 lines in history table; 1 - last index in history table.
 Rate: 1000000 Kbps, Packet size: 68 Bytes,
 Priority: 0, Tos: 0
 10 packets transmitted; 10 packets received, 0.00% packet loss  Round-trip min/avg/max:
11.616/11.800/11.888 us  Jitter min/avg/max: 0.000/0.028/0.256 us  Last good probe: Wed Jul
14 17:12:36 2010
OS900(config-rfc2544)#
```

# Layer 3 Testing

## Basic Steps

The basic steps for configuring and running a Layer 3 RFC 2544 test are:

- Creating an Inband VLAN interface on each of the two OS900s between which the test is to be run
- Creating a Test with default parameter values
- Defining the Destination IP Address for the Test
- Setting the Rate of the datastream
- Running the test

The procedures for changing the default parameter values are given in the section *Optional Configuration Parameters for Tests*, page *490*.

| | **Note** |
|---|---|
| | To run a test that has been created for Layer 2 at Layer 3, make sure that no Layer 2 setting is present in its configuration! |

## Creating an Inband VLAN Interface

At each of the two OS900s:

1. Create a Inband VLAN Interface as described in the section *Configuring*, page *181*.
2. In the Inband VLAN Interface mode, invoke the command **ip sla**.

## Creating a Test (or Entering its Mode)

To create a test with default parameter values and/or to enter its mode:

1. Enter **configure terminal** mode
2. Invoke the command:

   **rfc2544 tester OWNER NAME**

   where,

   **OWNER**: Owner name (e.g., Jojo)

   **[NAME]**: Test name (e.g., Test-1). Default: *

Example

```
OS912C(config)# rfc2544 tester OWNER_1 Test-1
OS912C(config-rfc2544)#
```

## Selecting the Type of Test

If the type of test is not selected, the ***Default*** test is run.

To select the type of test:

1. Enter the mode of the test.
2. Invoke the command:

   **test default|throughput**

   where,

   **default**: Default test.

   **throughput**: Throughput test.

Example

```
OS912C(config-rfc2544)# test throughput
OS912C(config-rfc2544)#
```

## Defining a Destination IP Address for a Test

To define a destination IP address for a test

1. Enter the mode of the Test.
2. Invoke the command:

   **dest-ip TARGET**

   where,

   **TARGET**: Target IP address or hostname.

Example

```
OS912C(config-rfc2544)# dest-ip 10.1.1.8
OS912C(config-rfc2544)#
```

## Setting the Rate of the Datastream

To set the rate of the datastream:

1. Enter the mode of the Test.

2. Invoke the command:
   **`rate RATELIMIT`**
   where,
   **`RATELIMIT`**: Rate of the data stream in bits per second.
   Range is 1 Kbps to 1 Gbps.
   In default test the rate of the sent test string is fixed.
   In throughput test the rate of the sent test string is the maximum.

Example

```
OS912C(config-rfc2544)# rate 3m
OS912C(config-rfc2544)#
```

To set the rate to zero (and therefore prevent running of the test) invoke the command **`no rate`**.

## Running a Test

To run a test:

1. Enter the mode of the test
2. Invoke the command:
   **`enable`**

Example

```
OS912C(config-rfc2544)# enable
OS912C(config-rfc2544)#
```

**Example**

--------------------------------------------RFC 2544 Test Configuration--------------------------------------------
(displayable as follows: `OS912C(config-rfc2544)#` **`show configuration`**)

```
!
! RFC 2544 Tester configuration
!
rfc2544 tester 1 1
 dest-ip  100.1.1.1
 rate 700m
 packets 100000
 test throughput
OS912C(config-rfc2544)#
```

--------------------------------Throughput Test for determining Lossless Rate--------------------------------

```
OS912C(config-rfc2544)# enable
OS912C(config-rfc2544)# Rate 700Mbps; loss 98.57%
Rate 350Mbps; loss 97.14%
Rate 175Mbps; loss 94.27%
Rate 87Mbps; loss 88.50%
Rate 43Mbps; loss 76.73%
Rate 21Mbps; loss 52.36%
Rate 10Mbps; loss 0.00%
Rate 15Mbps; loss 33.32%
Rate 12Mbps; loss 16.67%
Rate 11Mbps; loss 9.08%
Test completed. Maximum rate: 10Mbps; packet length: 68B

OS912C(config-rfc2544)# show
----------- type:tester owner:'1' testname:'1' stopped
length:           88      packets:        100
ttl:             128      timeout:        200 ms
history-size:     10      interval:       1000 us
dest-ip:      100.1.1.2
Resolved target: 100.1.1.2
Started at Tue Jun 30 20:16:56 2009
5 lines in history table.
Priority: 0, Tos: 0
100 packets transmitted; 100 packets received, 0.00% packet loss
Round-trip min/avg/max: 14.672/14.720/14.800 us
Jitter min/avg/max: 0.000/0.000/-0.080 us
```

```
Last good probe: Tue Jun 30 20:17:46 2009

--------------------------------------------Configuration and Last Result--------------------------------------------

----------- type:tester owner:'1' testname:'1' stopped
length:           88      packets:        100
ttl:             128      timeout:        200 ms
history-size:     10      interval:       1000 us
dest-ip:      100.1.1.2
Resolved target: 100.1.1.2
Started at Tue Jun 30 20:16:56 2009
5 lines in history table.
Priority: 0, Tos: 0
100 packets transmitted; 100 packets received, 0.00% packet loss
Round-trip min/avg/max: 14.672/14.720/14.800 us
Jitter min/avg/max: 0.000/0.000/-0.080 us
Last good probe: Tue Jun 30 20:17:46 2009

-----------------------------------------------Histories of Two Tests-----------------------------------------------

OS912C(config-rfc2544)# show rfc2544 history
----- Resolved target: 100.1.1.1-----
 Started at Sun May 28 22:35:59 2000
 Rate:  700000 Kbps, Packet size: 68 Bytes
 100000 packets transmitted; 1433 packets received, 98.57% packet loss
 Round-trip min/avg/max: 13.568/13.639/13.696 us
 Jitter min/avg/max: 0.000/-0.000/-0.112 us

----- Resolved target: 100.1.1.1-----
 Started at Sun May 28 22:36:02 2000
 Rate:  350000 Kbps, Packet size: 68 Bytes
 100000 packets transmitted; 2865 packets received, 97.14% packet loss
 Round-trip min/avg/max: 13.568/13.639/13.728 us
 Jitter min/avg/max: 0.000/0.000/-0.128 us
OS912C(config-rfc2544)#
```

# Stopping a Test

To stop a test before its completion:

1. Enter the mode of the test by invoking the command:
   **rfc2544 tester OWNER NAME**
   where,
   **OWNER**: Owner name (e.g., Jojo)
   **[NAME]**: Test name (e.g., Test-1). Default: *
2. Invoke the command:
   **no enable**

Example

```
OS912C(config-rfc2544)# no enable
OS912C(config-rfc2544)#
```

# Viewing Test Results

## RFC 2544 History

To view the history of a test:

1. Enter the mode of the test:
2. Invoke the command:
   **show rfc2544 history**

## Configuration Information on Tests

To view run-time RFC 2544 information for tests.

1. Enter the mode of the test.
2. Invoke the command:

**show configuration**

# Optional Configuration Parameters for Tests

This section provides procedures for changing parameter values of a test.
To change a parameter value, first enter the mode of a test.

## Service Level (SL)

To set the SL for a test, invoke the command:

**sl <1-8>**

where,

**<1-8>**: SL to be selected from the range 1 to 8

To reset the SL for a test to the default value (**1**), invoke the command:

**no sl**

## Description for a Test

### Adding/Replacing

To add/replace a textual description of a test:

1. Enter the mode of the test.
2. Invoke the command:

   **description ..**

   where,

   **description**: Textual description.

   **..**: Textual description.

Example

```
OS912C(config-rfc2544)# description Sales Dept.
OS912C(config-rfc2544)#
```

### Deleting

To delete the textual description of a test:

1. Enter the mode of the test.
2. Invoke the command:

   **no description**

Example

```
OS912C(config-rfc2544)# no description
OS912C(config-rfc2544)#
```

## Number of History Entries

### Custom

To limit the number of most recent history entries to be stored for a test:

1. Enter the mode of the test.
2. Invoke the command:

   **history-size <2-65535>**

   where,

   **<2-65535>**: Maximum number of history entries to be recorded from the range 2 to 65535. Default: **5**

Example

```
OS912C(config-rfc2544)# history-size 47
OS912C(config-rfc2544)#
```

#### Default

To reset the number of history entries to the default value (**5**):

1. Enter the mode of the test.
2. Invoke the command:
   **no history-size**

Example
```
OS912C(config-rfc2544)# no history-size
OS912C(config-rfc2544)#
```

### Rate-Change Size

This configuration parameter applies only for the *throughput test* type.

#### Custom

To set an increment whose multiples will be used to adjust the datastream rate each time before running the test in order to determine the maximum rate for which the packet loss is less than the selected % described in the section *Percentage Loss*, page *491*:

1. Enter the mode of the test.
2. Invoke the command:
   **step STEP**

   where,
   **STEP**: Increment size. Default: **1m** (1 Mbps)

Example
```
OS904(config-rfc2544)# step 3m
OS904(config-rfc2544)#
```

#### Default

The default increment is 1 Mbps. To set the increment to the default value (**1m**):

1. Enter the mode of the test.
2. Invoke the command:
   **no step**

Example
```
OS904(config-rfc2544)# no step
OS904(config-rfc2544)#
```

### Percentage Loss

This configuration parameter applies only for the *throughput test* type.

#### Custom

To set the maximum permitted % loss acceptable in determining the maximum datastream rate for such a loss:

1. Enter the mode of the test.
2. Invoke the command:
   **loss-ratio <0-100>**

   where,
   **<0-100>**: Allowed loss in %. Default: **0** (0 %).

Example
```
OS904(config-rfc2544)# loss-ratio 2
OS904(config-rfc2544)#
```

#### Default

The default loss is 0 %. To set the loss to the default value (**0**):

1. Enter the mode of the test.
2. Invoke the command:
   **no loss-ratio**

Example

```
OS904(config-rfc2544)# no loss-ratio
OS904(config-rfc2544)#
```

## Duration of Test

Since the duration and the number of packets for a test (see the section *Number of Packets*, page *492*) are interdependent, selecting one automatically resets the other.

#### Custom

To set the time (in seconds) during which the test is to run:

1. Enter the mode of the test.
2. Invoke the command:
   **duration <1-3600>**

   where,

   **<1-3600>**: Test duration in seconds. Default: **0**, i.e., the parameter *Number of Packets* (page *492*) is to be used instead of the parameter *Duration of Test* (page *492*).

Example

```
OS912C(config-rfc2544)# duration 274
OS912C(config-rfc2544)#
```

#### Default

To reset the time interval to the default value (**0**):

1. Enter the mode of the test.
2. Invoke the command:
   **no duration**

Example

```
OS912C(config-rfc2544)# no duration
OS912C(config-rfc2544)#
```

## Number of Packets

Since the number of packets and the duration of a test (see the section *Duration of Test*, page *492*) are interdependent, selecting one automatically resets the other.

#### Custom

To set the number of packets to be sent during each burst interval for a test:

1. Enter the mode of the test.
2. Invoke the command:
   **packets <1-1000000>**

   where,

   **<1-1000000>**: Number of packets to be sent to be selected from the range 1 to 1,000,000. Default: **3**.

Example

```
OS912C(config-rfc2544)# packets 561
OS912C(config-rfc2544)#
```

### Default

To reset the number of packets to be sent to the default value (**3**):

1. Enter the mode of the test.
2. Invoke the command:
   **no packets**

Example

```
OS912C(config-rfc2544)# no packets
OS912C(config-rfc2544)#
```

## Packet Length

### Custom

To set the packet length (includes L2VPT [802.1p] field bits and CRC) for a test that will help diagnose faults sensitive to this length:

1. Enter the mode of the test.
2. Invoke the command:
   **length <64-9216>**

   where,

   **<64-9216>**: Packet length (in octets) to be selected from the range 64 to 9216. Default: **68**

Example

```
OS912C(config-rfc2544)# length 3001
OS912C(config-rfc2544)#
```

### Default

To reset the Packet length to the default value (**68**):

1. Enter the mode of the test.
2. Invoke the command:
   **no length**

Example

```
OS912C(config-rfc2544)# no length
OS912C(config-rfc2544)#
```

## Data Pattern

### Adding

To add a data pattern (inside a packet) that will help to diagnose faults sensitive to incompleteness of data in a packet for a test:

1. Enter the mode of the test.
2. Invoke the command:
   **pattern HEXLINE**

   where,

   **HEXLINE**: Pattern (dataFill) of DataTLV using hexadecimal digits, e.g., **0123fa9c**. The number of characters must be an integral multiple of 8.

   If the packet length is greater than the pattern size, the pattern is repeated until the total length is equal to the packet size.

   If the packet length is less than the pattern size, the pattern is truncated to the packet length.

Example

```
OS912C(config-rfc2544)# pattern 6a029f3c
OS912C(config-rfc2544)#
```

### Deleting

To delete the data pattern:

1. Enter the mode of the test.
2. Invoke the command:
   **no pattern**

Example

```
OS912C(config-rfc2544)# no pattern
OS912C(config-rfc2544)#
```

## Layer 2 Packet Priority

### Custom

To set the L2VPT (802.1p) field bits for and accompanying a test:

1. Enter the mode of the test.
2. Invoke the command:
   **priority [<0-7>]**

   where,

   **[<0-7>]**: Layer 2 Packet priority to be selected from the range 0 (lowest priority) to 7 (highest priority). Default: **0**.

Example

```
OS912C(config-rfc2544)# priority 4
OS912C(config-rfc2544)#
```

### Default

To reset the Layer 2 Packet priority to the default value (**0**):

1. Enter the mode of the test.
2. Invoke the command:
   **no priority**

Example

```
OS912C(config-rfc2544)# no priority
OS912C(config-rfc2544)#
```

## Timeout

### Custom

To set the maximum wait time for test completion (msec):

1. Enter the mode of the test.
2. Invoke the command:
   **timeout <1-60000>**

   where,

   **<1-60000>**: Wait time (in milliseconds) from the range 0 to 60000. Default: **200**.

Example

```
OS912C(config-rfc2544)# timeout 3207
OS912C(config-rfc2544)#
```

### Default

To reset the wait time to the default value (**200**):

1. Enter the mode of the test.
2. Invoke the command:

**`no timeout`**

Example

```
OS912C(config-rfc2544)# no timeout
OS912C(config-rfc2544)#
```

## Time-To-Live

### Custom

To set the time-to-live for IP packets:

1. Enter the mode of the test.
2. Invoke the command:
   **`ttl <1-255>`**

   where,

   **`<1-255>`**: Time-to-live for IP packets from the range 1 to 255. Default: **`128`**.

Example

```
OS912C(config-rfc2544)# ttl 98
OS912C(config-rfc2544)#
```

### Default

To reset the time-to-live to the default value (**`128`**):

1. Enter the mode of the test.
2. Invoke the command:
   **`no ttl`**

Example

```
OS912C(config-rfc2544)# no ttl
OS912C(config-rfc2544)#
```

## DiffServ ToS (DSCP)

### Custom

To change the value of the IP ToS field that accompanies the test packet:

1. Enter the mode of the test.
2. Invoke the command:
   **`tos <0-255>`**

   where,

   **`<0-255>`**: ToS value from the range 0 to 255. Default: **`0`**.

Example

```
OS912C(config-rfc2544)# tos 203
OS912C(config-rfc2544)#
```

### Default

To set the value of the IP ToS field that accompanies the test packet to the default (**`0`**):

1. Enter the mode of the test.
2. Invoke the command:
   **`no tos`**

Example

```
OS912C(config-rfc2544)# no tos
OS912C(config-rfc2544)#
```

## Performance Monitoring Thresholds

### Invoking

#### *Frame-Delay/Jitter*

To set the performance monitoring thresholds for *frame-delay* or *jitter* for averages in a burst that will cause alarms to be sent to the CLI or SNMP manager when crossed:

1. Enter the mode of the test.
2. Invoke the command:
   **`threshold (frame-delay|jitter) rise <0-100000> fall <0-100000>`**

   where,

   **`frame-delay`**: Frame delay

   **`jitter`**: Jitter

   **`rise`**: Rise threshold

   **`<0-100000>`**: (First appearance) Rise threshold value to be selected from the range **`0-100000`**. It is the maximum time in microseconds *above* which an alarm is sent.

   **`fall`**: Fall threshold

   **`<0-100000>`**: (Second appearance) Fall threshold value to be selected from the range **`0-100000`**. It is the minimum time in microseconds *below* which an alarm is sent. This value must not exceed the *Rise* threshold value.

Example

```
OS904-DSL4(config-rfc2544)# threshold frame-delay rise 250 fall 200
OS904-DSL4(config-rfc2544)#
```

#### *Packet-Loss*

To set the performance monitoring thresholds for *packet-loss* for averages in a burst that will cause alarms to be sent to the CLI or SNMP manager when crossed:

1. Enter the mode of the test.
2. Invoke the command:
   **`threshold packet-loss rise <0-100> fall <0-100>`**

   where,

   **`packet-loss`**: Packet loss

   **`rise`**: Rise threshold

   **`<0-100>`**: (First appearance) *Rise* threshold value to be selected from the range **`0-100`**. It is the % packet loss *above* which an alarm is sent. This alarm indicates *impermissible* packet loss.

   **`<0-100>`**: (Second appearance) *Fall* threshold value to be selected from the range **`0-100`**. It is the % packet loss *below* which an alarm is sent. This alarm indicates *permissible* packet loss. The *Fall* threshold value must be *less than* the *Rise* threshold value.

Example

```
OS904-DSL4(config-rfc2544)# threshold packet-loss rise 36 fall 35
OS904-DSL4(config-rfc2544)#
```

### Revoking

To revoke the performance monitoring thresholds, invoke the command:

**`no threshold (frame-delay|jitter|packet-loss) [rise] [NUMBER] [fall] [NUMBER]`**

where,

**`frame-delay`**: Frame delay

**`jitter`**: Jitter

**`packet-loss`**: Packet loss

**[rise]**: Rise threshold
**[NUMBER]**: Rise threshold value
**[fall]**: Fall threshold
**[NUMBER]**: Fall threshold value

Example

```
OS904-DSL4(config-rfc2544)# no threshold frame-delay
OS904-DSL4(config-rfc2544)#
```

# Resetting all Parameters of a Test

To reset all parameters of a test to their default values:

1. Enter the mode of the test.
2. Invoke the command:
   **default**

Example

```
OS912C(config-rfc2544)# default
OS912C(config-rfc2544)#
```

# Clearing Statistics on a Test

To clear all statistics on a test:

1. Enter the mode of the test.
2. Invoke the command:
   **clear statistics**

Example

```
OS912C(config-rfc2544)# clear statistics
OS912C(config-rfc2544)#
```

# Chapter 27: Scheduler

## Definition

The scheduler function of the OS900 is used to schedule execution of administrator-specified commands at times pre-set by the administrator. The command types may be CLI or Linux. A CLI command may be a regular command or a script[69].

## Purpose

The scheduler allows the administrator to ensure that certain actions by/on the OS900 will be performed at the *right time* and *automatically*.

Examples of uses of the scheduler are: reboot the OS900 at the end of the day, load a new configuration at a pre-specified time, etc.

## Types of Scheduler Commands

There are four types of scheduler commands:

- Single-Execution
- Periodic-Execution
- Extended
- No-Execution
- Show Scheduler Configuration

These types of scheduler commands can be CLI or Linux commands.

To execute these commands, first enter the **`configure terminal`** mode as shown below:

```
OS900 login: admin
Password:
Last login: Wed Jun  8 09:24:24 2006 on ttyS0
Welcome to MRV's distribution for MPC8245.
OS900> enable
OS900# configure terminal
```

## Scope

If the type of a *Single-Execution*, *Periodic-Execution*, or *Extended* scheduler command is CLI, it is required to belong to **`enable`** mode.

The *execution time* for these scheduler commands can be set to within a 1-minute margin.

The *Single-Execution* and *Periodic-Execution* scheduler commands provide for sending event notification following execution.

The *Single-Execution* scheduler command is used to execute a command just once.

The *Periodic-Execution* scheduler command is used to execute a command periodically as follows:

- Every minute
- Every hour at a specific minute
- Every day at a specific hour and minute
- Every month on a specific day and at a specific hour and minute
- At a specific day of the week (e.g., Sunday) every month or a specific month at a specific hour and minute

[69] A script is a set of CLI commands that the OS900 can execute in succession without user intervention. For details, refer to the section *Scripts*, page *118*.

The *Periodic-Execution* scheduler command cannot be used to execute a command periodically if the period is in the range:

– 2 and 59 minutes (e.g., every 2 minutes)

– 2 and 23 hours (e.g., every 2 hours)

– 2 or more days (except 7, because it can be executed every weekday)

– 2 or more months

The *Extended* scheduler command has more capability than the *Periodic-Execution* scheduler command. It can be used to execute a command periodically for any period (e.g., every 2 minutes). Further, unlike the *Single-Execution Scheduler Command* and *Periodic-Execution Scheduler Command*, several (up to 65535) such scheduler commands can be pre-configured concurrently for execution.

# Single-Execution Scheduler Command

## Purpose

This type of scheduler command causes execution of a CLI or Linux command just once.

## Syntax

The command syntax is as follows:

**`schedule once MONTH DAY TIME [notifying] (cli|linux) COMMAND`**

where,

**`MONTH`**: Month (e.g., **`June`**) during which the command is to be executed. Either type the full name of the month or at least the first three letters (e.g., **`Jun`**). In any case, the month name must begin with capital (upper case) letter.

**`DAY`**: Day (e.g., **`27`**) on which the command is to be executed. The day can be any number in the range **`1-31`**, provided the day is valid for the month. (For e.g., 31 for the month of June is *not* valid.)

**`TIME`**: Time (e.g., **`13:15`**) at which the command is to be executed. The time must typed in the following format:

**`HH:MM`**

where,

**`HH`**: Hour as a 2-digit number.

The hour can be any number in the range **`0-23`**.

**`MM`**: Minute as a 2-digit number.

The minute can be any number in the range **`0-59`**.

**`[notifying]`**: Send event notification following execution of the scheduling command.

**`(cli|linux)`**: Choice between **`cli`** and **`linux`**.

**`cli`** is *CLI* command type.

**`linux`** is *Linux* command type.

**`COMMAND`**: The specific CLI or Linux command to be executed by the OS900. If the command type is CLI, it is required to belong to **`enable`** mode.

Example 1:

In order to cause a configuration to be saved on June 15 at the time 23 hr and 51 min, invoke the following CLI command:

**`schedule once Aug 7 23:51 cli write file`**

Example 2:

In order to cause the OS900 to reboot on December 7 at the time 18 hr and 35 min, invoke the following CLI command:

**`schedule once Dec 7 18:35 cli reboot-force`**

# Periodic-Execution Scheduler Command

## Purpose

This type of scheduler command causes periodic execution of CLI or Linux commands.

## Syntax

The command syntax is as follows:

**`schedule period MINUTE HOUR DAY MONTH WDAY [notifying] (cli|linux) COMMAND`**

where,

`MINUTE`: Minute at which the command is to be executed.
Either type:

– A number in the range `0-59`, e.g., `43`
Or
– `*` for execution every minute.

`HOUR`: Hour at which the command is to be executed.
Either type:

– A number in the range `0-23`, e.g., `16`
Or
– `*` for execution every hour.

`DAY`: Day on which the command is to be executed.
Either type:

– A number in the range `1-31`, e.g., `27`. (For example, `31` for the month of February, April, June, etc. is *not* valid since each of these months has less than 31 days!)
Or
– `*` for execution every day.

`MONTH`: Month during which the command is to be executed.
Either type:

– The full name of the month (e.g., `June`) or at least the first three letters (e.g., `Jun`). In any case, the month name must begin with capital (upper case) letter.
Or
– `*` for execution every month.

`WDAY`: Day of the week on which the command is to be executed.
Either type:

– The full name of the weekday (e.g., `Sunday`)
Or
– `*` for ignoring what day it is of the week.

**`[notifying]`**: Send event notification following execution of the scheduling command.
**`(cli|linux)`**: Choice between **`cli`** and **`linux`**.
**`cli`** is *CLI* command type.
**`linux`** is *Linux* command type.

`COMMAND`: The specific CLI or Linux command to be executed by the OS900. If the command type is CLI, it is required to belong to **`enable`** mode.

| **Note** |
| --- |
| In selecting the values for **`MONTH`** and **`WDAY`**, make sure that they are compatible according to the calendar! |

Example

In order to cause the OS900 configuration to be saved on the FTP server whose IP address is **`195.90.123.5`** in the directory **`c:/config_bak`** every day at the time **`23`** hr and **`0`** min, invoke the following CLI command:

**`schedule period 00 23 * * * cli copy startup-config ftp 195.90.123.5 c:/config_bak`**

# Extended Scheduler Command

## Purpose

This type of scheduler command is used to cause execution of a CLI or Linux command once, several times, or periodically.

## Configuration

### Setup

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`schedule extended <1-65535>|new`**
   where,
   **`<1-65535>`**: Range of schedule IDs from which one is to be selected by the user.
   **`new`**: Schedule ID to be selected by the OS900. The OS900 assigns the highest ID in the range that is available. For e.g., if **`65535`** and **`65533`** are assigned and **`65534`** is available, the use of the argument **`new`** will assign the ID **`65534`** to the next scheduler command that is set up.
3. Invoke the command:
   **`command cli|linux COMMAND`**
   where,
   **`cli`**: CLI command type.
   **`linux`**: Linux command type.
   **`COMMAND`**: The specific CLI or Linux command to be executed by the OS900. If the command type is CLI, it is required to belong to **`enable`** mode.

   **`enable`** mode.
4. Invoke the command:
   **`interval <1-527040>`**
   where,
   **`<1-527040>`**: Interval between two consecutive command executions in minutes.
5. Invoke the command in one of the following two options:
   Option 1: Number of times command is to be executed.
   **`number-of-times <1-527040>`**
   where,
   **`<1-527040>`**: Number of times command is to be executed.
   Option 2: Time by which the schedule will stop.
   **`end-time forever|(MONTH DAY TIME)`**
   where,
   **`forever`**: Schedules the command to run indefinitely.
   **`MONTH`**: The Month (e.g., **`March`**, **`*`** for this month).

**`DAY`**: The day (e.g., **`10`**, **`*`** for this day).

**`TIME`**: The time (e.g., **`13:15`**).

6. Set the time at which the schedule can start by invoking the command:

   **`start-time now|(MONTH DAY TIME)`**

   where,

   **`now`**: The schedule is to start immediately.

   **`MONTH`**: The Month (e.g., **`March`**, **`*`** for this month).

   **`DAY`**: The day (e.g., **`10`**, **`*`** for this day).

   **`TIME`**: The time (e.g., **`13:15`**).

7. (Optional) Add a user comment on the scheduler command by invoking the command:

   **`remark STRING`**

   where,

   **`STRING`**: User comment on the scheduler command. The comment may be up to 132 characters long.

### Enabling

A scheduler command can be enabled for execution only after it has been set up as described in the section *Setup*, page *502*, just above.

To enable execution of a scheduler command that has already been set up:

1. Enter **`configure terminal`** mode.
2. Enter the mode of the scheduler command that is to be enabled by invoking the command:

   **`schedule extended <1-65535>`**

   where,

   **`<1-65535>`**: Range of schedule IDs from which the ID of the scheduler command that is to be enabled must be selected.
3. Invoke the command:

   **`enable`**

### Example 1

In this example, running of loopback test is configured. The test starts on the **`20`**th of **`November`** at **`13:15`**, will be run every hour (**`60`** minutes) indefinitely.

```
schedule extended 1
  remark run loopback test with burst of 10 frames
  start-time Nov 20 13:15
  end-time forever
  interval 60
  command cli ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 10
  enable
```

### Example 2

In this example too, running of loopback test is configured. However, the test is set to start immediately, will run every hour in the **`3`** following hours.

```
schedule extended 2
  remark run loopback test with burst of 10 frames
  start-time now
  number-of-times 3
  interval 60
  command cli ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 10
  enable
```

**Notes**

1. In case of conflicting configuration commands, for example, **`end-time forever`** and **`number-of-times <1-527040>`**, the last command is reinforced.
2. If entry configured to “start-time now” and “enable”, then in case of device reset, the scheduler will run the scheduled command immediately, even if it had been completed before the reset.
3. The old extended scheduler entry format is supported only from start up configuration.

# Viewing

## All Configured Scheduler Commands

### In Brief

To view all the configured scheduler commands *in brief*:

1. Enter **`enable`** mode.
2. Invoke the command
   **`show schedule`**

Example

```
OS900(config)# show schedule
Schedule table is empty.
Id     Enable Complete Start-time   End-time     Number   Interval Type Command
==========================================================================
1      Yes    No       Nov 20 13:15 Forever      -        60       cli  etherne
2      Yes    No       Now          -            3        60       cli  etherne
OS900(config)#
```

### In Detail

To view all the configured scheduler commands *in detail*:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show schedule extended details`**

Example

```
OS900# show schedule extended details
Shedule 1 details:
-------------------
Enable         : Yes
Complete       : No
Start-time     : Nov 20 13:15
End-time       : Forever
Number of times: -
Interval       : 60
Command type   : cli
Command        : ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 1

Shedule 2 details:
-------------------
Enable         : Yes
Complete       : No
Start-time     : Now
End-time       : -
Number of times: 3
Interval       : 60
Command type   : cli
Command        : ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 1
OS900#
```

## Specific Configured Scheduler Command

### Method 1

To view a specific configured scheduler command:

1. Enter **enable** mode.
2. Invoke the command:

   **show schedule extended details [INDEX]**

   where,

   **[INDEX]**: ID (in the range **<1-65535>**) of the scheduler command about which information is to be viewed.

Example

```
OS900# show schedule extended details 1
Shedule 1 details:
-------------------
Enable         : Yes
Complete       : No
Start-time     : Nov 20 13:15
End-time       : Forever
Number of times: -
Interval       : 60
Command type   : cli
Command        : ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 1
OS900#
```

### Method 2

1. Enter **configure terminal** mode.
2. Invoke the command:

   **schedule extended <1-65535>**

   where,

   **<1-65535>**: Range of schedule IDs from which one is to be selected by the user.
3. Invoke the command:

   **show scheduler**

Example

```
OS900# configure terminal
OS900(config)# schedule extended 1
OS900(sched-1)# show scheduler
  remark run loopback test with burst of 10 frames
  start-time Nov 20 13:15
  end-time forever
  interval 60
  command cli ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 10
  enable
OS900(sched-1)#
```

### Run-time Configuration of Extended Scheduler Commands

To view the run-time configuration of extended scheduler commands:

1. Enter **enable** mode.
2. Invoke the command:

   **show running-config schedule extended**

Example

```
OS900# show running-config schedule extended
schedule extended 1
  remark run loopback test with burst of 10 frames
  start-time Nov 20 13:15
  end-time forever
  interval 60
  command cli ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 10
  enable
schedule extended 2
  remark run loopback test with burst of 10 frames
  start-time now
  number-of-times 3
  interval 60
  command cli ethernet oam domain 4 service 1 mep 1000 loopback rmep 2000 10
  enable
OS900#
```

# OAM Operation Scheduler Command

To schedule an IEEE 802.1ag or ITU-T SG 13 Y.1731 standard OAM operation, use the command described in the section *Automatic Scheduling of Delay Measurement, Loopback, and Link Trace*, page *420*.

# No-Execution Scheduler Command

### Purpose

This type of scheduler command cancels a scheduled command.

### Syntax

The command syntax is as follows:

**no schedule COMMAND**

where,

**COMMAND** – Specific CLI or Linux command to be canceled.

Example

In order to stop the saving of the OS900 configuration on the FTP server whose IP address is 195.90.123.5 in the directory c:/config_bak every day (at the time 23 hr and 0 min), invoke the following CLI command:

**`no schedule copy startup-config ftp 195.90.123.5 c:/config_bak`**

# Show Scheduler Configuration Command

## Purpose

This type of scheduler command shows the commands that will be executed by the scheduler.

## Syntax

The command syntax is as follows:

**`show schedule [COMMAND]`**

where,

**`[COMMAND]`** – (optional) The specific CLI or Linux command schedule to be viewed. If the argument is typed, all arguments of this scheduled command will be shown. If the argument is *not* typed, all defined scheduled commands and their arguments will be shown.

Below is an example showing two schedules.

```
OS900(config)# show schedule
Complete Month Day Weekday   Hour Min Type  Notif Command
========================================================
No         Aug 7             23   51  cli         write file
No         Aug 7             23   58  cli         reboot
End Of Schedule Table
OS900(config)#
```

The entry `No` in the column `Complete` means the command has not been executed. After the command is executed, '`No`' changes to '`Yes`.'

# **Chapter 28:** Transparent-Mode Media Cross-Connect

## General

The Media Cross-Connect application provides it with *intelligent* patchpanel-like functionality. In typical patchpanels, wires must be physically disconnected, moved, and reconnected to change the network configuration. In the OS900, (and herein lies its great advantage) physical connections are left unchanged; only logical connections are changed – purely by software control – to give the desired port-to-port interconnections.

One application of Media Cross-Connect is to forward data via a WDM technology port.

## Principle of Operation

Media Cross-Connect allows the administrator to program the OS900 to forward traffic entering one user-specified port to another or to flood another user-specified port *group* – in transparent mode. In this mode, the forwarding is done like that by a repeater; fully transparently (i.e., with no MAC address learning and no processing).

*Figure 44*, below, illustrates Media Cross-Connect.

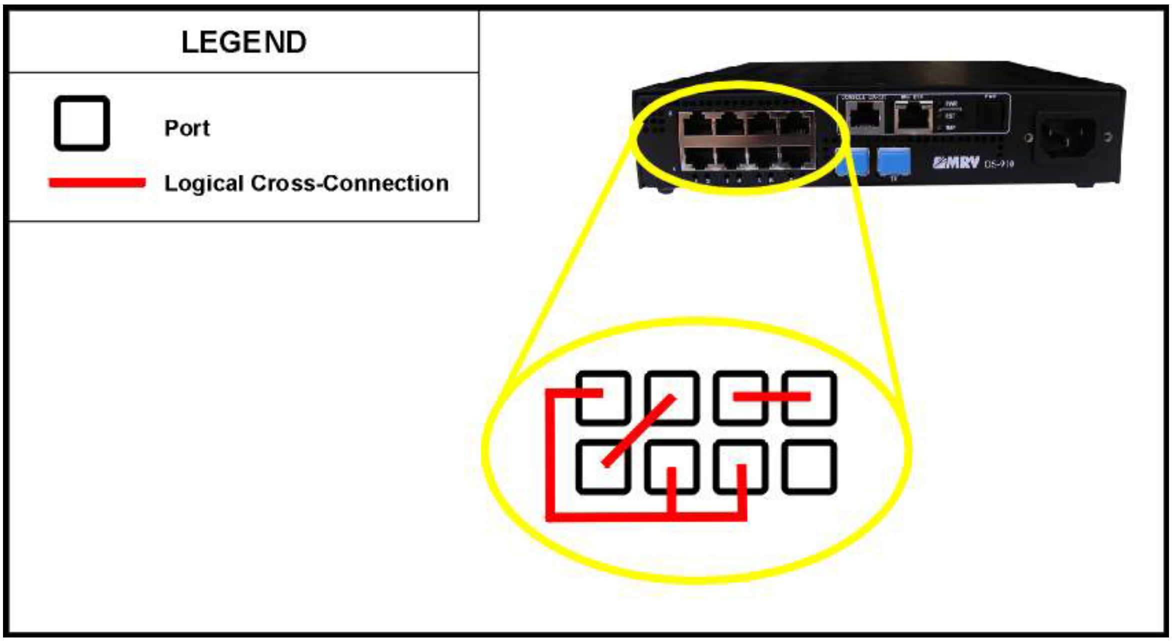



**Figure 44: Media Cross-Connection Examples in the OS900**

## Examples

Example 1

The example below shows how to configure Media Cross-Connection between ports 3 and 4.

```
OS900(config)# port tag-outbound-mode q-in-q 3-4 20
OS900(config)# interface vlan vif20
OS900(config-vif20)# tag 20
OS900(config-vif20)# ports 3-4
OS900(config-vif20)# exit
OS900(config)# no port lt-learning 3-4
OS900(config)#
```

Example 2

This example shows use of a script to program media cross-connect.

```
OS900(config)# script cross-connect

OS900(script-cross-connect)# parameter 10   ID type vifN description IF for X-connect
OS900(script-cross-connect)# parameter 20   POID type ports description Ports for X-connect

OS900(script-cross-connect)# line      20   port tag-outbound-mode q-in-q $POID $ID
OS900(script-cross-connect)# line      30   interface vlan vif$ID
OS900(script-cross-connect)# line      40   tag $ID
OS900(script-cross-connect)# line      50   ports $POID
OS900(script-cross-connect)# line      60   no port lt-learning $POID

OS900(script-cross-connect)# write terminal
Building configuration...

Current configuration:
! version 1-0-0
!
script cross-connect
 parameter 10   ID type vifN description IF for X-connect
 parameter 20   POID type ports description Ports for X-connect
line      20   port tag-outbound-mode q-in-q $POID $ID
 line      30   interface vlan vif$ID
 line      40   tag $ID
 line      50   ports $POID
 line      60   no port lt-learning $POID
!
OS900(script-cross-connect)# exit
OS900(config)# exit

OS900# cross-connect ?
  <1-4095>   cross-connect_ID(range:2-4095)
OS900# cross-connect 20 ?
  PORT_GROUP_STR  cross-connect_ports(e.g 2-3)
OS900# cross-connect 20 8-10
execute: port tag-outbound-mode q-in-q 3-4
execute: interface vlan vif20
execute: tag 20
execute: ports 3-4
Interface is activated.
execute: no port lt-learning 3-4 entries 0
OS900#
```

Example 3

This example shows how to configure an OS900 to function as a 2-port media converter (transparent cross-connect switch) that is completely transparent to customer tagged and untagged frames and that can be managed inband with tagged management packets.

```
Current configuration:
! version 2_1_2
!
access-list extended port3
 rule 10
  action redirect port 4
  action tag nest 1000
!
access-list extended port4
 rule 10
  action permit
  tag eq 127
 rule 20
```

```
  action redirect port 3
  action tag nest 1000
!
port tag-outbound-mode hybrid 3-4 1000
!
port acl-binding-mode by-port 3-4
port access-group port3 3
port access-group port4 4
!
interface vlan vif127
 description management
 tag 127
 ip 11.1.0.1/24
 ports 4
!
interface vlan vif1000
 description MediaConverter
 tag 1000
 ports 3-4
!
```

# Chapter 29: Firmware Viewing and Upgrading/Downloading

## General

This chapter provides general information on the:

– OS900 image (operative-program firmware)

– FPGA firmware

And shows how to upgrade/download an OS900 image, and how to reboot the OS900 so that it runs with the new firmware.

The image, containing the executable code that runs on the OS900, is preinstalled at the factory in the OS900 storage device in compressed form. The OS900 automatically decompresses the file before activating the image. The image should be upgraded as new versions are released. For the latest image, you can: Contact your local MRV representative, E-mail us at InternationalSupport@mrv.com, or Visit our MRV Web site at http://www.mrv.com

The image is upgraded using a download procedure from a File Transfer Protocol (FTP) server on the network.

The OS900 storage device has the following partitions:

– 2 partitions for firmware images (current, backup)

– 2 partitions for configuration files (current, backup) – see ***Chapter 30: Configuration*** , page *519*.

During upgrading/downloading of a new image, the partition *that does not contain the image being run* is formatted and the new image is downloaded in a backup store there. The boot sector is then updated in such a way that at the next boot the image in the backup store becomes the *current* OS900 image. As part of the upgrade procedure the relevant configuration files are upgraded without affecting the custom configurations.

## Requirements

To upgrade/download the OS900 image from a version that is lower than 1.0.11 to version 3.1.4, the OS900 image must first be upgraded to version 1.0.11. The image must then be run (by rebooting) and only then the version 1.0.11 can be upgraded to version 3.1.4. You can use the procedure given below without Step *5* to upgrade to 1.0.11.

In order to upgrade an OS900 unit to firmware version 3.1.4 (or later), its associated activation key is required. To receive the activation key, email your request to MPLS@mrv.com.

## Downloading a New Image

To upgrade/download a new image:

1. Load the new image onto an FTP remote directory on your network (if you will be using FTP).
2. Log into the OS900.
3. Enter **`enable`** mode.
4. Download the new image to the OS900 using either of the following commands:

    **`upgrade [force-reboot|no-reboot] ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]`**

    **`upgrade [force-reboot|no-reboot] scp SERVER REMOTE-DIR REMOTE-FILENAME USERNAME PASSWORD`**

    where,

    **`ftp`**: Upgrade using FTP protocol.

**`force-reboot`**: Reboot automatically following successful upgrade. (This optional argument is used so that step *7* below can be skipped.)

**`no-reboot`**: Do not reboot following successful upgrade. (This optional argument is used so that step *7* below can be skipped.)

**`FTP-SERVER`** or **`SERVER`**: Host name or IP address of the FTP server containing the image to be downloaded.

**`REMOTE-DIR`**: Full path to the directory containing the image on the FTP server.

**`REMOTE-FILENAME`**: Name of the image file in the directory.

**`USERNAME`**: Name of the user authorized to access the FTP server.

**`PASSWORD`**: Password for accessing the FTP server.

(Alias **`copy ftp firmware`**: **`VERSION FTP-SERVER REMOTE-DIR [USERNAME] [PASSWORD]`**

**`scp`**: Upgrade using secure copy from server.

5. In response to the prompt:
   `Enter activation key recieved from MRV:`
   Type in the activation key (12-characters long)
6. Wait until the completion of the upgrade process, which may last a few minutes.
7. In response to the prompt (if it appears)
   `Would you like to reboot the system now ? (y|n)`
   Type **`y`** if you want to run the new image now.
   Type **`n`** if you want to run the new image later and let the previous image keep running in the meantime.
   The new image can be run at any time as described in the section *Rebooting*, page *110*.

If the upgrade/download process fails (for e.g., due to an FTP problem or illegal compressed file), the OS900 runs the previous image.

| | **Note** |
|---|---|
| | Powering the OS900 off and on will also run the new image. |

To revert to the previous image, use the procedure described in the section *Rerunning the Previous Image*, page *515*.

Example

```
OS900# upgrade ftp 10.90.136.241 pub OS900-1-0-4.ver

Please wait for ftpget to finish ...

Check route to 10.90.136.241
Netmask = 255.255.0.0
FTP file pub/OS900-1-0-4.ver from 10.90.136.241 user  password  ...
Transferring data: 19815kB 100%
FTP Succeed
Write image to Flash...
Erasing blocks: 156/156 (100%)
Writing data: 19896k/19896k (100%)
Verifying data: 19896k/19896k (100%)
Copy & Merge configuration files...
Switch to boot partition 1
Would you like to reboot the system now? (y|n)
y
The system is rebooting !!!
Stopping internet superserver: xinetd.
Stopping periodic command scheduler: cron.
Stopping OpenBSD Secure Shell server: sshd.
Stopping portmap daemon: portmap.
```

```
Saving random seed... done.
Stopping kernel log daemon: klogd.
Stopping system log daemon: syslogd.
The system is going down NOW !!
Sending SIGTERM to all procesha exited !!!
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
Restarting system.

OS900#
```

# Rerunning the Previous Image

## General

The OS900 has two images. One image is stored on memory partition number 1, the other on 3. When booting, the U-BOOT software reads one of the boot parameters (identified as **`bootpart`**) in order to determine the partition from which to boot.

Upgrade/download causes the new image to be written to the partition that was not used at boot, i.e., to the one the OS900 is not currently running. At the end of the upgrade procedure, the OS900 modifies the **`bootpart`** value to enable the *new* image to be run following reboot.

In order to rerun the previous image, the **`bootpart`** value must be changed to the previous value.

**`bootpart`** can have the value 1 or 3 corresponding to the partitions. If the value is 1, you need to change it to 3, and vice versa.

## Procedure

The procedure for changing the **`bootpart`** value is as follows:

(For security reasons, this procedure *cannot* be performed using a remote connection, e.g., TELNET, SSH, or SNMP.)

1. Connect a craft terminal (e.g., PC with an ASCII terminal emulation software application) to the OS900 **CONSOLE EIA-232** port with a Serial/RS-232 line as described in the section *Craft Terminal/Emulator (For Out-of-band Management)*, page *81*.
2. Boot or reboot the OS900.
3. As soon as the following first lines of U-BOOT initialization appear on your terminal:

```
U-Boot 1.1.1 (Apr 18 2004 - 16:11:20)

CPU:   MPC8245 Revision 1.4 at 266.666 MHz: 16 kB I-Cache 16 kB D-Cache
I2C:   ready
DRAM:  256 MB
Board: MRV SBC Revision: 1.1 Serial Number: 0000000001
FLASH: 68 MB
```

   Type:

   **`stop`**, and press Enter.

   The boot sequence will stop, and the U-BOOT prompt => is displayed.
4. Type:

   **`printenv`**, and press Enter.

   Typically, the following information is displayed.

```
ethaddr=00:0F:BD:00:05:B8
ethact=i82559#0
bootfile=uImage
bootretry=5
bootdelay=3
bootm
ramboot=chpart $(bootpart); fsload $(bootfile); run flashargs addmisc; bootm
```

```
flashargs=setenv bootargs root=/dev/mtdblock1 bootpart=$(bootpart)
nfsargs=setenv bootargs root=/dev/nfs rw nfsroot=$(serverip):$(rootpath)
addip=setenv bootargs $(bootargs) ip=$(ipaddr):$(serverip):$(gatewayip):$(netmas
k):$(hostname):$(netdev):off
addmisc=setenv bootargs $(bootargs) console=ttyS0,$(baudrate)
gatewayip=10.90.136.254
netmask=255.255.255.0
ipaddr=192.168.1.10
serverip=192.168.1.20
rootpath=/home/eyalm/ppc_root/
baudrate=9600
bootcmd=run ramboot
bootpart=1
stdin=serial
stdout=serial
stderr=serial
cpuid=1
hwver=1
boardsn=0000000001

Environment size: 797/65531 bytes
=>
```

5. Check the **bootpart** value. (The example display, above, shows **bootpart=1**.)
6. Change the **bootpart** value to the other (i.e., if it is 1 change it to 3, and vice versa) using the command:
   **set bootpart 3**
7. Save the configuration using the command:
   **saveenv**

   Typically, the following information is displayed.

```
Saving Environment to Flash...
Un-Protected 1 sectors
Un-Protected 1 sectors
Erasing Flash...
. done
Erased 1 sectors
Writing to Flash... done
Protected 1 sectors
Protected 1 sectors
=>
```

8. Reset the OS900 using command:
   **reset**

The OS900 will now boot from partition 3.

# Running the Backup Image

The version of the backup image of the OS900 can be viewed using the procedure given in the section *Backup Image*, page *107*.

To set the OS900 to operate with the Backup Image:

1. Enter **enable** mode.
2. Invoke the command:
   **reboot|reboot-force backup**
   **reboot** if you want to reconsider whether to reboot.
      In response to the prompt:
      `Would you like to reboot the system from backup partition now? (y|n)`
      Type **y** if you want to reboot with the Backup Image now.
      Type **n** if you do *not* want to reboot.
   Or

**reboot-force** if you want rebooting with the Backup Image to be done straightaway, i.e., without prompts.

# FPGA

## Applicability

FPGA applies only to the OS904, OS906, and OS912 models.

## Viewing Firmware Versions

To view the firmware version running the FPGA and the firmware version that can be downloaded to run the FPGA:

1. Enter **enable** mode.
2. Invoke the command:
   **show fpga version**

Example

```
OS900# show fpga version
Current FPGA version: FirmWare version - 0x9
SW version file that stored for FPGA module: rev9.bit
OS900#
```

In the example above:

– The firmware version currently running the FPGA is marked in red.
  If the firmware has been corrupted, `0x0` will appear instead to indicate that firmware has to be downloaded to the FPGA.

– The file containing firmware for upgrading the FPGA is marked in blue.
  This FPGA File is a temporary file, i.e., it is deleted following reboot of the OS900. It can also be deleted as described in the section *Deleting File*, page *518*.
  It appears in the OS900 only after it has been copied as described in the section *Copying Firmware*, just below. It is only used to upgrade the FPGA.

## Copying Firmware

To copy the FPGA firmware[70] from an FTP server to the FPGA File (temporary) in the OS900, invoke the command:

**copy ftp fpga FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]**

where,

**FTP-SERVER**: Hostname of the FTP server (or IP address)

**REMOTE-DIR**: Full path to the directory containing the FPGA firmware on the FTP server.

**REMOTE-FILENAME**: Name of the FPGA File in the directory.

**USERNAME**: Name of the user authorized to access the FTP server.

**PASSWORD**: Password for accessing the FTP server.

Example

```
OS900# copy ftp fpga 10.90.136.153 pub rev9.bit
/usr/local/nbase/bin/copy_ethoam_fpgaver.sh 10.90.136.153 pub rev9.bit
Check route to 10.90.136.153
Netmask = 255.255.255.0
```

[70] This firmware can optionally be used, at a later stage, to replace the existing firmware running the FPGA.

```
FTP file pub/rev9.bit from 10.90.136.153 user  password...
FTP Succeed
OS900#
```

## Upgrading Firmware

Upgrading the FPGA will cause the old firmware version to be overwritten with the new one.
Before performing upgrade:

1. Enter **configure terminal** mode
2. Disable all scheduler commands set to perform OAM actions by entering the modes of the commands and invoking the command:
   **no enable**
3. Disable Ethernet OAM by invoking the command:
   **no ethernet oam enable**

To run the FPGA with the firmware version stored in the FPGA File, invoke the command:
**upgrade fpga**

Example

```
OS900# upgrade fpga
FPGA version successfully upgraded.
OS900#
```

To upgrade the FPGA from an SNMP Manager, refer to the *MegaVision User Manual*.

## Deleting File

To delete the FPGA File, invoke the command:
**remove fpga-file**

Example

```
OS900# remove fpga-file
OS900#
```

# Chapter 30: Configuration Management

## General

A configuration file consists of a set of configuration CLI commands that were executed on the OS900. As configuration settings are changed, the new settings get stored in run-time memory. The settings in run-time memory are not retained when the OS900 is rebooted. To retain the settings in the OS900, they must be copied to the flash (permanent) memory as described in the section *Saving Run-time Configuration to the Startup Configuration File*, page *520*.

## Viewing Configuration Files

### Available

To view the available configuration files, invoke the command:

**show file**

Example

```
OS900# show file
drwxrwxrwx    2 admin    admin         140 Dec 25 14:13 .
drwxrwxrwx    4 root     admin         200 Dec 25 14:11 ..
-rw-rw----    1 admin    admin      231538 Dec 23 17:58 1000vc
-rwxrwxrwx    1 root     admin        7709 Dec 25 10:59 System.conf
-rw-rw----    1 admin    admin        7709 Dec 25 14:13 koko
-rwxrwxrwx    1 root     admin      231538 Dec 23 17:57 kuku
OS900#
```

### Current

To view the configuration file currently in use, invoke the command:

**show boot-config-file**

Example

```
OS900# show boot-config-file
boot config file:  /usr/local/etc/sys/System.conf
OS900#
```

## Selecting a New Configuration File

To select a new configuration file, invoke the command:

**boot-config-file FILE**

where,

**FILE**: Name of the file to be used to configure the OS900.

Example

```
OS900# boot-config-file System.conf
Changes will take place after reboot
OS900#
```

## Deleting a Configuration File

To delete a configuration file, invoke the command:

**delete conf NAME**

Example

```
OS900# delete conf koko
OS900#
```

# Saving *Run-time* Configuration to the *Startup* Configuration File

To save the *run-time* configuration (in RAM) to the *Startup* Configuration File (in flash permanent memory), use any one of the following methods:

## Method 1

1. Enter **enable** mode or any other mode under it.
2. Invoke the following command:
   **write file [NAME]**
   where,
   **[NAME]**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **system.conf**.

Example

```
OS900# write file
Building Configuration...
[OK]
OS900#
```

## Method 2

1. Enter **enable** mode or any other mode under it.
2. Invoke the following command:
   **write memory**

Example

```
OS900# write memory
Building Configuration...
[OK]
OS900#
```

## Method 3

1. Enter **enable** mode or any other mode under it.
2. Invoke the following command:
   **copy running-config startup-config**
   where,
   **running-config**: Copy from Run-time configuration file.
   **startup-config**: Copy to Startup configuration file.

Example

```
OS900# copy running-config startup-config
Building Configuration...
[OK]
OS900#
```

# Saving *Startup* Configuration to the Backup Partition

To save the *Startup* Configuration (in flash permanent memory) to the *Backup* Partition (also in flash permanent memory):

1. Enter **enable** mode.

2. Invoke the following command:
   **`copy startup-config backup-partition`**

Example

```
OS900# copy startup-config backup-partition
Wait please, copying and merging the configuration files...
Copying and merging configuration files ended successfully.
OS900#
```

# Viewing Configuration Information

To view all the configuration information on the management console, enter **`enable`** mode or any other mode under it, and invoke the command:

**`write terminal`**

Example

```
OS900# write terminal
Building configuration...

Current configuration:
! version 1-0-4
!
port flood-limiting rate 2m 1,2
port flood-limiting rate 16.96m 3,4
port flood-limiting multicast 3,4
port flood-limiting tcp-syn 4
!
port tag-outbound-mode tagged 1-2
!
interface vlan vif7
!
interface vlan vif10
 tag 980
 ports 1-2
!
interface vlan vif20
 tag 20
 ip 23.0.0.3/24
 ports 3-4
 management
!
interface vlan vif100
!
interface out-of-band eth0
 ip 10.90.136.38/24
 management
!
spanning-tree
 enable
!
OS900(config)#
```

# Restoration of Factory Default Configuration

To restore the factory default configuration to the OS900 (and to save the current configuration):

1. Enter the **`enable`** mode.
2. Invoke the command:
   **`write erase`**

Example

```
OS900# write erase
Restore factory defaults and backup current configuration.
Ok.
OS900#
```

To make the factory default configuration run-time, invoke the command **`reboot`**.

# Restoration of Erased Configuration

To restore the OS900 configuration that existed prior to erasure by the command **`write erase`**:

1. Enter the **`enable`** mode.
2. Invoke the command:
   **`write old-configuration`**

Example

```
OS900> enable
OS900# write old-configuration
Restore last erased configuration.
OS900#
```

This action will delete all the user-configurations performed *after* the command **`write erase`** was invoked.

# Configuration Files Upload/Download

## General

A configuration file consists of a set of configuration CLI commands that were executed on the OS900. As configuration settings are changed, the new settings get stored in run-time memory. The settings in run-time memory are not retained when the OS900 is rebooted. To retain the settings in the OS900, they must be copied to the flash (permanent) memory as described in the section *Saving Run-time Configuration to the Startup Configuration File*, page *520*.

This chapter describes how to copy (upload or download) an OS900 configuration file in one of the following ways:

– Upload (copy Startup configuration file to FTP/SSH Server)

– Download (copy configuration file from FTP/SSH Server to Startup configuration file)

## Upload

The Startup Configuration File in the OS900 can be uploaded to an FTP server on your network. The uploaded file is ASCII coded and retains the CLI format. Once the file is uploaded, you can:

- Modify the configuration using a text editor, and later download a copy of the file to the same OS900, or to one or more other OS900s.
- Send a copy of the configuration file to the MRV Customer Support Department for troubleshooting.
- Automatically upload the configuration file periodically, e.g., each day, each week, etc., so that the FTP server can archive the configuration. (The procedure for setting the OS900 to schedule periodic upload of the configuration – or any other CLI command action – is described in ***Chapter 27:*** *Scheduler*, page *499*.)

To copy the *Startup* configuration file to an *FTP or SSH Server*:

1. Enter **`enable`** mode.
2. Invoke the command in either of the following methods:
   Method 1: (*Without Encryption using FTP*)
   **`copy startup-config ftp FTP-SERVER REMOTE-DIR [remote-file FILENAME] [USERNAME] [PASSWORD]`**

where,

**`copy`**: Copy file.

**`startup-config`**: *From* Startup configuration.

**`ftp`**: *To* FTP server.

**`FTP-SERVER`**: DNS Host name or IP address of the FTP server.

**`REMOTE-DIR`**: Full pathname to the directory on the FTP server.

**`[remote-file FILENAME]`**: Name for the file to which the startup configuration is to be copied and which is to be uploaded to the remote server.

**`[USERNAME]`**: Username for FTP login.

**`[PASSWORD]`**: Password for FTP login.

Method 2: (*With Encryption using Secure Copy*)

**`copy startup-config scp SERVER REMOTE-DIR USERNAME PASSWORD [FILENAME]`**

where,

**`copy`**: Copy file.

**`startup-config`**: *From* startup configuration.

**`scp`**: *To* SSH server.

**`SERVER`**: DNS Host name or IP address of the server.

**`REMOTE-DIR`** Full pathname to the directory on the server.

**`USERNAME`**: Username for login.

**`PASSWORD`**: Password for login.

**`[FILENAME]`**: Name for the file to which the startup configuration is to be copied and which is to be uploaded to the remote server.

Example

```
OS900> enable
OS900# copy startup-config ftp 10.83.132.65 ./configurations Zorro Mypassword
OS900#
```

## Download

To copy a configuration file that is on an *FTP/SSH Server* to the *Startup* configuration file:

1. Enter **`enable`** mode.
2. Invoke the command in either of the following methods:

Method 1: (*Without Encryption using TELNET*)

**`copy ftp startup-config FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]`**

where,

**`copy`**: Copy file.

**`ftp`**: *From* FTP server.

**`startup-config`**: *To* Startup configuration file.

**`FTP-SERVER`**: DNS Host name or IP address of the FTP server.

**`REMOTE-DIR`**: Full pathname to the directory on the FTP server.

**`REMOTE-FILENAME`**: Filename in the directory on the FTP server.

**`[USERNAME]`**: Username for FTP login.

**`[PASSWORD]`**: Password for FTP login.

Method 2: (*With Encryption using SSH*)

**`copy scp startup-config SERVER REMOTE-DIR REMOTE-FILENAME USERNAME PASSWORD`**

where,

**`copy`**: Copy file.

**`scp`**: *From* SSH server.

**`startup-config`**: *To* Startup configuration file.

**`SERVER`**: DNS Host name or IP address of the server.

**`REMOTE-DIR`**: Full pathname to the directory on the server.

**`REMOTE-FILENAME`** Filename in the directory on the server.

**`USERNAME`**: Username for login.

**`PASSWORD`**: Password for login.

To make the downloaded configuration file run-time, reboot the OS900 using the command **`reboot`**.

Example

```
OS900> enable
OS900# copy ftp startup-config 10.83.132.65 ./Configurations MyFile Zorro Mypass
OS900# reboot
```

Another way to back up IP configuration files stored in the OS900 is to use the procedure given in the section *TFTP Server Mode*, page *179*, for the out-of-band Ethernet interface (***MGT ETH***) or in the section *TFTP Server Mode*, page *192*, for inband VLAN Ethernet interfaces.

# **Chapter 31:** Dynamic Host Configuration Protocol (DHCP)

## General

DHCP is an IP protocol that enables management of a network by automatically giving each host an IP address for a specific duration of time, called 'lease time'. The lease time determines how long an IP address remains valid for a host in the network, the default being one day. Using DHCP, network clients can be supplied dynamically with leased IP addresses for varying lease times.

The device that leases these IP addresses is called a DHCP server. In some networks, the DHCP server and the hosts may be on different subnets. In such case, the DHCP server can be accessed only via an intermediary agent called a DHCP relay. A DHCP relay sends DHCP requests from one subnet to one or more DHCP servers on other subnets.

## OS900 Operation Modes

The OS900 can operate with DHCP in one or *both* of the following modes:

- Server Mode
- Relay Mode
- Snooping Mode
- Client Mode

### Server Mode

#### General

In Server Mode, the OS900 functions as a DHCP server. The administrator can specify OS900 interfaces at which the OS900 will listen for DHCP requests.

#### Setting

To set the OS900 in DHCP *Server Mode*:

1. Directing DHCP Requests to the CPU

   In order to prevent DoS attacks, the OS900, by default, blocks non-ARP broadcasts to the CPU. To enable DHCP broadcast requests to reach the DHCP server (or relay), the packets must be explicitly trapped to the CPU using an ACL.

   The procedure for enabling DHCP broadcasts requests to reach the OS900 set as a DHCP server (or relay) is as follows:

   1.1. Create an extended ACL using the command:

   **`access-list extended WORD`**

   where,

   **`WORD`**: Name of the ACL

   1.2. Create a rule as follows:

   a. Create a rule that characterizes the packet as being of *UDP* protocol, with destination port *DHCP server* (67), and destination MAC address type *broadcast* using the commands:

   **`rule [RULE_NUM]`**

   where,

   **`[RULE_NUM]`**: (optional) Index of rule. If this argument is not entered, the rule is indexed automatically, i.e., it gets a number that is a multiple of 10. This number is the smallest that is larger than the highest in the group of rules created for the ACL.

**protocol eq udp**

**dest-port eq 67**

where,

**67**: DHCP server port

**source-ip eq 0.0.0.0/32**

b. Select the action that traps packets to the CPU using the command:

**action trap-to-cpu**

1.3. Set the default policy to *permit* packet forwarding (in case no rule applies for the packet type) using the command:

**default policy permit**

1.4. Bind the ACL to *each* interface for which DHCP broadcast packets are to be trapped to the CPU using the command:

**access-group WORD**

where,

**WORD**: ACL name

2. Enter the following modes in succession:

   **enable → configure terminal → dhcp**

3. Enter the VLAN interface ID at which the OS900 will listen for DHCP requests or the Subnet IP address/mask of the OS900 by invoking the command:

   **entry IFNAME|SUBNET/MASK**

   where,

   **IFNAME**: VLAN interface ID at which the OS900 will listen for DHCP requests.

   **SUBNET/MASK**: Subnet IP address/mask of the OS900. The mask can be up to 31 bits long.

4. Enter the range of IP addresses from which the OS900 is to allocate addresses to clients by invoking the command:

   **range LOWER-RANGE [UPPER-RANGE]**

   where,

   **LOWER-RANGE**: Lower limit of range of IP addresses from which the OS900 is to allocate addresses to clients

   **UPPER-RANGE**: Upper limit of range of IP addresses from which the OS900 is to allocate addresses to clients

5. (Optional) Set the IP Default Gateway and Subnet Mask for the host by invoking the following commands:

   **router ROUTER_IP**

   where,

   **ROUTER_IP**: IP address of Default Gateway for host

   **subnet-mask MASK**

   where,

   **MASK**: IP address *mask* for host. The mask can be up to 31 bits long.

6. (Optional) Set the Domain Name to be published by the OS900 by invoking the command:

   **domain DOMAIN_NAME**

   where,

   **DOMAIN_NAME**: Domain Name to be published by the OS900. It identifies one or more hostnames. Examples of domain names are *mrv.com* and *worldcharity.org*. An example of a hostname belonging to the domain *mrv.com* is *torro.mrv.com*. Every domain name has a suffix that indicates the Top-Level Domain (TLD) to which it belongs. In the examples above, the domain name suffixes are *com* and *org*.

(To *revoke* the above command, use the prefix **no** with the command.)

7. (Optional) Enter the IP address of the OS900 to be used by DHCP clients by invoking the following command.
   **dns SERVER_IP**
   where,
   **SERVER_IP**: IP address of the OS900
8. (Optional) Set the maximum lease time allowed for any client by invoking the command:
   **max-lease-time TIME**
   where,
   **TIME**: Maximum lease time (in seconds). Any value in the range **1** to **2147483646** may be selected. Selecting **0** will set the maximum lease time to the default value, **86400**.
   (To *revoke* the above command, use the prefix **no** with the command.)
9. (Optional) Set the lease time that will be allotted to clients who do not specify the lease time by invoking the command:
   **default-lease-time TIME**
   where,
   **TIME**: Default lease time (in seconds). Default: 86400 seconds. (This time must not exceed the maximum lease time.)
   (To *revoke* the above command, use the prefix **no** with the command.)
10. (Optional) If a separate log file for the DHCP server log messages is to be assigned, invoke the command:
    **separate-log**
11. (Optional) To enable the OS900 to perform the '*NetBIOS over TCP/IP Name Server*' function of the NetBIOS service, invoke the command:
    **netbios name-server IP_ADDRESS**
    where,
    **IP_ADDRESS**: IP address of the NetBIOS name server
    For more than one name server, repeat the above command for each name server in order of preference.
12. (Optional) To enable the OS900 to perform the '*NetBIOS over TCP/IP Node Type*' function of the NetBIOS service, invoke the command:
    **netbios node-type NODETYPE**
    where,
    **NODETYPE**: **1** (B-node), **2** (P-node), **4** (M-node), or **8** (H-node).
13. Enable DHCP Server Mode for the OS900 by invoking the command:
    **enable**
    (To *revoke* the above command, use the prefix **no** with the command.)

### Viewing

To view DHCP server configuration details:

1. Enter **enable** mode or **dhcprelay** mode.
2. Invoke the command:
   **show dhcp**

To print out the DHCP file showing the leases, invoke the command:

**show dhcp leases**
where,
**leases**: Print out the DHCP file showing the leases.

### Example

```
MRV OptiSwitch 910 version 2_0_10
OS910 login: admin
Password:
```

```
OS910> enable
OS910# configure terminal

     ---------------Creating an ACL that will trap DHCP packets to the CPU-------------

OS910(config)# access-list extended toCPU
OS910(config-access-list)# default policy permit
OS910(config-access-list)# rule 10
OS910(config-rule)# action trap-to-cpu
OS910(config-rule)# protocol eq udp
OS910(config-rule)# source-ip eq 0.0.0.0/32
OS910(config-rule)# dest-port eq 67
OS910(config-rule)# exit
OS910(config-access-list)# exit

     ----------Creating VLAN interfaces and binding the ACL to the interfaces----------

OS910(config)# interface vlan vif80
OS910(config-vif80)# ports 6-9
OS910(config-vif80)# tag 108
Interface is activated.
OS910(config-vif80)# ip 169.2.2.3/24
OS910(config-vif80)# access-group toCPU
OS910(config-vif80)# exit

     -------------------------------Setting Server Mode-------------------------------

OS910(config)# dhcp

OS910(config-dhcp)# entry vif80
OS910(config-dhcp-subnet)# range 169.2.2.5 169.2.2.114
OS910(config-dhcp-subnet)# exit

OS910(config-dhcp)# max-lease-time 604800 (1 week)
OS910(config-dhcp)# default-lease-time 86400 (1 day)
OS910(config-dhcp)# enable

     --------------------Viewing DHCP Server configuration details---------------------

OS910(config-dhcp)# show dhcp
DHCP CONFIGURATION:
 default lease time = 86400
 max lease time = 604800
 entry: device = vif80
              range: 169.2.2.5     169.2.2.114
 dhcp status = enable
OS910(config-dhcp)#
```

## Relay Mode

### General

In Relay Mode, the OS900 functions as a *DHCP relay*. The user can specify separate OS900 interfaces for the servers and clients.

### Setting

To set the OS900 in DHCP *Relay Mode*:

1. Enable DHCP packets to be trapped to the CPU by performing the procedure described in Step *1*, page *525*.
2. Enter the following modes in succession:
   **`enable`** → **`configure terminal`** → **`dhcprelay`**
3. For each DHCP server to be accessed, invoke the command:
   **`server IP_ADDRESS`**

   where,
   **`IP_ADDRESS`**: IP address of server

   (To *revoke* the above command, use the prefix **`no`** with the command.)

| | |
|---|---|
| | **Note**<br>Either perform both Steps *4* and *5* (below) or skip them. If you skip them, *all* the IP interfaces of the OS900 will be listened on for DHCP requests. |

4. Define one or more interfaces at which *server* replies are to be received by invoking the command:
   **`entry IFNAME`**
   where,
   **`IFNAME`**: ID of DHCP *server* interface having the format **`vifX`**, where **`X`** is a decimal number in the range **`1-4095`**.
   (To *revoke* the above command, use the prefix **`no`** with the command.)
5. Define one or more interfaces at which DHCP *client* requests are to be forwarded by invoking the command:
   **`entry IFNAME`**
   where,
   **`IFNAME`**: ID of DHCP *client* interface having the format **`vifX`**, where **`X`** is a decimal number in the range **`1-4095`**.
   (To *revoke* the above command, use the prefix **`no`** with the command.)

| | |
|---|---|
| | **Note**<br>The OS900 does not assign the interfaces defined in steps *4* and *5*, above, to the servers and clients. The relays and clients must be configured to connect to these interfaces. |

6. (Optional) Option 82

   The DHCP Relay Agent Information Option (No. 82) – described in RFC 3046 – can be activated in the OS900 set in DHCP Relay Mode. This option enables the OS900 to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information (e.g., OS900 physical port for DHCP communication) to implement policies for assignment of parameter values (e.g., IP address).

   To activate Option 82 in the OS900 (set in DHCP Relay Mode), invoke the command:
   **`option82`**
   (To *revoke* the above command, invoke the command **`no option82`**.)
7. Enable DHCP Relay Mode for the OS900 by invoking the command:
   **`enable`**

(To *revoke* the above command, use the prefix **no** with the command.)

**Viewing**

To view DHCP relay configuration details:

1. Enter **enable** mode or **dhcprelay** mode.
2. Invoke the command:
   **show dhcprelay**

**Example**

Following is an example demonstrating configuration of the OS900 as a DHCP relay.

```
MRV OptiSwitch 910 version 2_0_10
OS910 login: admin
Password:

OS910> enable
OS910# configure terminal

     ---------------Creating an ACL that will trap DHCP packets to the CPU-------------

OS910(config)# access-list extended toCPU
OS910(config-access-list)# default policy permit
OS910(config-access-list)# rule 10
OS910(config-rule)# action trap-to-cpu
OS910(config-rule)# protocol eq udp
OS910(config-rule)# source-ip eq 0.0.0.0/32
OS910(config-rule)# dest-port eq 67
OS910(config-rule)# exit
OS910(config-access-list)# exit

     ----------Creating VLAN interfaces and binding the ACL to the interfaces----------

OS910(config)# interface vlan vif50
OS910(config-vif50)# ports 6,7
OS910(config-vif50)# tag 30
Interface is activated.
OS910(config-vif50)# ip 192.168.1.2/24
OS910(config-vif50)# access-group toCPU
OS910(config-vif50)# exit

OS910(config)# interface vlan vif60
OS910(config-vif60)# ports 8-10
OS910(config-vif60)# tag 40
Interface is activated.
OS910(config-vif60)# ip 192.168.10.88/24
OS910(config-vif60)# access-group toCPU
OS910(config-vif60)# exit

     --------------------------------Setting Relay Mode-------------------------------

OS910(config)# dhcprelay
OS910(config-dhcprelay)# server 192.168.1.1
OS910(config-dhcprelay)# entry vif50
OS910(config-dhcp-subnet)# exit
OS910(config-dhcprelay)# entry vif60
OS910(config-dhcp-subnet)# exit
OS910(config-dhcprelay)# option82
OS910(config-dhcprelay)# enable

     --------------------Viewing DHCP Relay configuration details---------------------

OS910(config-dhcprelay)# show dhcprelay
```

```
 Listening on interface  vif50
 Listening on interface  vif60
 Forward to server: 192.168.1.1
 dhcprelay - running
OS910(config-dhcprelay)#
```

## Snooping Mode

### General

Snooping Mode can be configured for an OS900 that is set in Relay Mode. Snooping enables the *DHCP server* to differentiate between clients. The user can specify separate OS900 interfaces for the servers and clients.

### Setting

To set the OS900 in DHCP *Snooping Mode*:

1. Make sure that the OS900 is set in Relay Mode. (The procedure is described in the section *Relay Mode*, page *529*).
2. Enable DHCP packets to be trapped to the CPU by performing the procedure described in Step *1*, page *525*.
3. Enter the following modes in succession:
   **enable → configure terminal → dhcp-snooping**
4. Specify the OS900 ports via which DHCP server configuration messages are to be accepted by invoking the command:
   **trust ports (PORT-GROUP|all)**
   where,
   **PORT-GROUP**: Group of ports to be trusted
   **all**: All ports to be trusted
   (To specify OS900 ports via which DHCP server configuration messages are to be *rejected*, invoke the command **no trust ports (PORT-GROUP|all)**.)
5. (Optional) To activate Option 82 (described in Step *6*, page *529*, above), invoke the command:
   **option82**
6. Enable DHCP Snooping Mode for the OS900 by invoking the command:
   **enable**
   (To *revoke* the above command, use the prefix **no** with the command.)

### Viewing

To view DHCP relay configuration details:

1. Enter **enable** mode or **dhcprelay** mode.
2. Invoke the command:
   **show dhcprelay**

### Example

Following is an example demonstrating configuration of the OS900 in Snooping Mode.

```
OS904(config)# dhcp-snooping
OS904(config-dhcp-snoop)# trust ports 1,3
OS904(config-dhcp-snoop)# option82
OS904(config-dhcp-snoop)# enable
OS904(config-dhcp-snoop)#
```

## Client Mode

### General

Each Inband VLAN Interface of the OS900 can be configured as an independent DHCP client.

### Activation

To activate an Inband VLAN Interface as a DHCP client:

1. Enter the mode of an existing Inband VLAN Interface by invoking the command:

   **`interface vlan IFNAME`**

   where,

   **`IFNAME`**: Interface ID having the format **`vifX`**, where **`X`** is a decimal number in the range 1-4095
2. To activate the Inband VLAN Interface as a DHCP client, invoke the command:

   **`ip dhcp`**

Example

```
OS904(config-vif8)# ip dhcp
IP DHCP already activated
OS904(config-vif8)#
```

### Deactivation

1. Enter the mode of an existing Inband VLAN Interface by invoking the command:

   **`interface vlan IFNAME`**

   where,

   **`IFNAME`**: Interface ID having the format **`vifX`**, where **`X`** is a decimal number in the range 1-4095
2. To deactivate the Inband VLAN Interface as a DHCP client, invoke the command:

   **`no ip dhcp`**

Example

```
OS904(config-vif8)# no ip dhcp
OS904(config-vif8)#
```

### Optional Configuration Parameters

#### *IP Address Acquisition*

Finite

To set a time limit for a response from the DHCP server to a request for an IP address by the OS900 for the Inband VLAN Interface:

1. Enter the mode of the Inband VLAN Interface.
2. Invoke the command:

   **`ip dhcp client timeout TIMEOUT`**

   where,

   **`TIMEOUT`**: Timeout in seconds. Default: **`60`**

Indefinite

To cause the OS900 to wait indefinitely for a response from the DHCP server to a request for an IP address by the OS900 for the Inband VLAN Interface:

1. Enter the mode of the Inband VLAN Interface.
2. Invoke the command:

   **`ip dhcp client timeout unlimited`**

Default

To reset the time limit (for a response from the DHCP server to a request for an IP address by the OS900 for the Inband VLAN Interface) to the default value (60 seconds):

1. Enter the mode of the Inband VLAN Interface.
2. Invoke the command:

```
no ip dhcp client timeout
```

***Broadcast Mode***

In this mode, the OS900 DHCP client is instructed to set the DHCP broadcast flag in its Discover and Request packets, so that it will always receive broadcast replies from servers.

Enabling

To enable this mode:

1. Enter the mode of the Inband VLAN Interface.
2. Invoke the command:
   ```
   ip dhcp client broadcast
   ```

Disabling

To disable this mode:

1. Enter the mode of the Inband VLAN Interface.
2. Invoke the command:
   ```
   no ip dhcp client broadcast
   ```

# Chapter 32: BOOTstrap Protocol (BOOTP)

## General

The OS900 can be set to operate in client mode with BOOTP. In this mode it can receive the following from a DHCP server:

- IP address for the OS900
- IP address of the remote TFTP server from which the configuration for the OS900 can be downloaded
- Name of the file on the remote TFTP server containing the configuration for the OS900

## Configuration

### IP Address only from DHCP Server Automatically

To set the OS900, do the following:

1. Create a VLAN interface via which BOOTP is to be run
2. Obtain an IP address for the OS900 from a DHCP server via the VLAN interface
3. Enter **`boot`** mode.
4. Invoke one or both of the following commands:

   <u>Enabling *In-band* Ethernet Ports to Receive IP Addresses</u>

   **`bootp VLAN-TAG PORTS TAGGED_PORTS`**

   where,

   **`VLAN-TAG`**: Tag of VLAN interface via which BOOTP is to be run

   **`PORTS`**: Ports of the VLAN interface via which BOOTP is to be run

   **`TAGGED_PORTS`**: Ports of the VLAN interface that are tagged. Enter 'none' if all ports are untagged

   <u>Enabling the *Out-of-band* Ethernet Port to Receive IP Addresses</u>

   To enable the **MGT ETH** port[71] to receive IP addresses from a BOOTP server, invoke the command:

   **`bootp eth0`**

To make the setting runtime

1. Save the settings in permanent memory by invoking the command **`write file`** or **`write memory`**.
2. Enter **`enable`** mode.
3. Invoke the command:

   **`reboot`**

   or

   **`reboot-force`**

### IP Address and Configuration File from DHCP Server Automatically

To set the OS900, do the following:

1. Create a VLAN interface via which BOOTP is to be run
2. Obtain an IP address for the OS900 from a DHCP server via the VLAN interface

---

[71] Out-of-band Ethernet 10/100Base-TX port for TELNET, SSH, and/or SNMP *out-of-band* connection and marked Management Ethernet Port in *Figure 2*, page *65*.

3. Obtain the configuration file for the OS900 from a DHCP server via the VLAN interface *automatically* (i.e., without specifying the TFTP server IP address or name of the configuration file)
4. Enter **`boot`** mode
5. Invoke one or both of the following commands:

   Enabling *In-band* Ethernet Ports to Receive IP Addresses and Configuration Files

   **`bootp VLAN-TAG PORTS TAGGED-PORTS get-cfg-via-tftp`**

   where,

   **`VLAN-TAG`**: Tag of VLAN interface via which BOOTP is to be run

   **`PORTS`**: Ports of the VLAN interface via which BOOTP is to be run

   **`TAGGED_PORTS`**: Ports of the VLAN interface that are tagged. Enter 'none' if all ports are untagged

   **`get-cfg-via-tftp`**: Get configuration file using TFTP

   Enabling the *Out-of-band* Ethernet Port to Receive IP Addresses

   To enable the **MGT ETH** port to receive IP addresses from a BOOTP server, invoke the command:

   **`bootp eth0`**

   Enabling the *Out-of-band* Ethernet Port to Receive Configuration Files

   **`bootp eth0 get-cfg-via-tftp CFG-FILENAME TFTP-SERVER`**

   where,

   **`CFG-FILENAME`**: Name of the configuration file located on the TFTP server

   **`TFTP-SERVER`**: Hostname or IP address of the TFTP server

To make the setting runtime

1. Save the settings in permanent memory by invoking the command **`write file`** or **`write memory`**.
2. Enter **`enable`** mode
3. Invoke the command:

   **`reboot`**

   or

   **`reboot-force`**

## IP Address only Automatically and Configuration File Manually from DHCP Server

To set the OS900, do the following:

1. Create a VLAN interface via which BOOTP is to be run
2. Obtain an IP address for the OS900 from a DHCP server via the VLAN interface
3. Obtain the configuration file for the OS900 from a DHCP server via the VLAN interface *manually* (i.e., by specifying the TFTP server IP address and name of the configuration file)
4. Enter **`boot`** mode
5. Invoke the command:

   Enabling *In-band* Ethernet Ports to Receive IP Addresses and Configuration Files

   **`bootp VLAN-TAG PORTS TAGGED-PORTS get-cfg-via-tftp CFG-FILENAME TFTP-SERVER`**

   where,

   **`VLAN-TAG`**: Tag of VLAN interface via which BOOTP is to be run

   **`PORTS`**: Ports of the VLAN interface via which BOOTP is to be run

   **`TAGGED_PORTS`**: Ports of the VLAN interface that are tagged. Enter 'none' if all ports are untagged

   **`get-cfg-via-tftp`**: Get configuration file using TFTP

   **`CFG-FILENAME`**: Name of configuration file on the TFTP server

**`TFTP-SERVER`**: TFTP server hostname or IP address

Enabling the *Out-of-band* Ethernet Port to Receive IP Addresses

To enable the **MGT ETH** port to receive IP addresses from a BOOTP server, invoke the command:

**`bootp eth0`**

Enabling the *Out-of-band* Ethernet Port to Receive Configuration Files

**`bootp eth0 get-cfg-via-tftp CFG-FILENAME TFTP-SERVER`**

where,

**`CFG-FILENAME`**: Name of the configuration file located on the TFTP server

**`TFTP-SERVER`**: Hostname or IP address of the TFTP server

To make the setting runtime:

1. Save the settings in permanent memory by invoking the command **`write file`** or **`write memory`**.
2. Enter **`enable`** mode
3. Invoke the command:

   **`reboot`**

   or

   **`reboot-force`**

## Bootup Configuration

By default, the OS900 assumes the configuration given in the **`system.conf`** file (located on the OS900) only when:

– It receives its IP address without the configuration from the DHCP server, or

– The timeout time (set as described in the section *Timeout Period*, page *538*) expires

### Enabling

To enable the OS900 to assume the configuration given in the **`system.conf`** file *as soon as the OS900 boots up*:

1. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
2. Invoke the command:

   **`bootp-option preload-config`**

Example

```
OS912C(config-boot)# bootp-option preload-config
BOOTP option would be activated from next boot
OS912C(config-boot)#
```

### Disabling

To disable the OS900 from assuming the configuration given in the **`system.conf`** file *as soon as the OS900 boots up*:

1. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
2. Invoke the command:

   **`no bootp-option preload-config`**

Example

```
OS912C(config-boot)# no bootp-option preload-config
BOOTP option erased, default value available from next boot
OS912C(config-boot)#
```

# Optional Configuration Parameters

## Timeout Period

### IP Address Acquisition

***Finite***

To set a time limit for a response from the BOOTP server to a request for an IP address by the OS900:

1. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
2. Invoke the command:
   **`bootp-option timeout TIMEOUT`**
   where,
   **`TIMEOUT`**: Timeout in seconds. Default: **`60`**

Example

```
OS912C(config-boot)# bootp-option timeout 75
BOOTP option would be activated from next boot
OS912C(config-boot)#
```

***Indefinite***

To cause the OS900 to wait indefinitely for a response from the BOOTP server to a request for an IP address by the OS900:

3. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
4. Invoke the command:
   **`bootp-option timeout unlimited`**

Example

```
OS912C(config-boot)# bootp-option timeout unlimited
BOOTP option would be activated from next boot
OS912C(config-boot)#
```

***Default***

To reset the time limit (for a response from the BOOTP server to a request for an IP address by the OS900) to the default value (60 seconds):

1. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
2. Invoke the command:
   **`no bootp-option timeout`**

Example

```
OS912C(config-boot)# no bootp-option timeout
BOOTP option erased, default value available from next boot
OS912C(config-boot)#
```

### Configuration File Acquisition

***Finite***

To set a time limit for a response from the TFTP server to a request for a configuration file by the OS900:

1. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
2. Invoke the command:
   **`bootp-option tftp-timeout TIMEOUT`**
   where,
   **`TIMEOUT`**: Timeout in seconds in the range 30 to 3600. Default: **`60`**.

Example

```
OS912C(config-boot)# bootp-option tftp-timeout 50
BOOTP option would be activated from next boot
OS912C(config-boot)#
```

***Default***

To reset the time limit for a response from the TFTP server (to a request for a configuration file by the OS900) to the default value (60 seconds):

1. Enter the following modes in succession: **enable** → **configure terminal** → **boot**.
2. Invoke the command:
   **no bootp-option tftp-timeout**

Example

```
OS912C(config-boot)# no bootp-option tftp-timeout
BOOTP option erased, default value available from next boot
OS912C(config-boot)#
```

## Retry Interval

This is a future option.

When BOOTP is activated for the OS900 it sends DHCP discover packets in order to acquire an IP address. If at the end of the timeout period (settable as described in the section *IP Address Acquisition*, page *538*) the OS900 does not receive an IP address, the DHCP client stops sending DHCP discover packets for a duration known as 'retry-interval'. At the end of the retry-interval, the OS900 sends another set of DHCP discover packets.

To set the retry-interval between consecutive sets of BOOTP/DHCP discover packets

1. Enter the following modes in succession: **enable** → **configure terminal** → **boot**.
2. Invoke the command:
   **bootp-option retry-interval RETRY_INTERVAL**
   Where,
   **RETRY_INTERVAL**: Time duration in seconds for which the DHCP client stops sending DHCP discover packets. Default: **300**.

## DHCP Client Activity

This is a future option.

If a BOOTP created interface is deleted while BOOTP is activate the OS900 DHCP client will keep dumping errors to the log file. To prevent such a scenario deactivate the OS900 DHCP client before erasing the BOOTP created interface.

### Deactivation

To deactivate the OS900 DHCP client:

1. Enter the **enable** mode.
2. Invoke the command:
   **bootp stop**

### Activation

To activate the OS900 DHCP client:

1. Enter the **enable** mode.
2. Invoke the command:
   **no bootp stop**

## Broadcast Mode

In this mode, the OS900 DHCP client is instructed to set the BOOTP broadcast flag in its Discover and Request packets, so that it will always receive broadcast replies from servers. To set this mode:

3. Enter the following modes in succession: **enable** → **configure terminal** → **boot**.
4. Invoke the command:
   **bootp-option broadcast-always**

Example

```
OS912C(config-boot)# bootp-option broadcast-always
BOOTP option would be activated from next boot
OS912C(config-boot)#
```

## Vendor ID

### *Enabling*

To enable the OS900 to send a user-defined vendor ID to the DHCP server whenever it attempts to access the DHCP server:

1. Enter the following modes in succession: **enable** → **configure terminal** → **boot**.
2. Invoke the command:
   **bootp-option vendor-class-identifier VENDOR_ID**
   where,
   **VENDOR_ID:** ID of the vendor. The ID may be any alphanumeric string without blank spaces (e.g., `MRV_OptiSwitch_912C`)

Example

```
OS912C(config-boot)# bootp-option vendor-class-identifier MRV_OptiSwitch_912C
BOOTP option would be activated from next boot
OS912C(config-boot)#
```

### *Disabling*

To disable the OS900 from sending a user-defined vendor ID to the DHCP server:

1. Enter the following modes in succession: **enable** → **configure terminal** → **boot**.
2. Invoke the command:
   **no bootp-option vendor-class-identifier**

Example

```
OS912C(config-boot)# no bootp-option vendor-class-identifier
BOOTP option erased, default value available from next boot
OS912C(config-boot)#
```

## Management

### Enabling

To enable management via the interface created for BOOTP (using any of the settings described in the section *Configuration*, page *535*):

1. Enter the following modes in succession: **enable** → **configure terminal** → **boot**.
2. Invoke the command:
   **bootp-option management**

**Disabling**

To disable management via the interface created for BOOTP (using any of the settings described in the section *Configuration*, page *535*):

1. Enter the following modes in succession: **`enable`** → **`configure terminal`** → **`boot`**.
2. Invoke the command:
   **`no bootp-option management`**

# Chapter 33: Network Time Protocol (NTP) and Timezone

## General

**N**etwork **T**ime **P**rotocol (NTP) is an Internet standard protocol (built on top of TCP/IP) for synchronizing clocks of network devices (PCs, routers, switches, etc.) to Standard Time (ST). ST is a combination of Universal Time (UT), zonetime, and summertime.

*UT* is the time for points located at longitude zero on the Earth (e.g., Greenwich). It is usually based on UTC[72]. UT can be accessed from any of a large number of NTP servers available on the Internet or GPS, for e.g., MRV's *NTP* server.

*Zonetime* is the number of hours offset from UT. It depends on the *zone* (geographical location) in which the device is located.

*Summertime* is an integral number of hours offset from the *zonetime*. It depends on whether it is currently in force for the country/zone.

Coded zonetime merged with summertime can be accessed from MRV's *FTP* server.

NTP runs in the background as a continuous client program sending periodic requests to the UT server for timestamps, which it uses to adjust the OS900's system clock.

The NTP versions (1, 2, or 3) running on the OS900 are based on RFC 1305. Version 3 is accurate to the millisecond.

## Configuration

To configure the OS900 to run NTP, do the following:

1. Enter **`configure terminal`** mode.
2. To set *any* zonetime, invoke the command:

   **`clock timezone NAME ABBREVIATION HH [0-59]`**

   where,

   **`NAME`**: Name for the time zone

   **`ABBREVIATION`**: Abbreviation for the time zone (e.g., GMT, E%sT, etc. '%s' is a 2-value variable. The value of the variable is automatically set and is displayed when the command **`show time`** is invoked as shown in the example below. The value of the variable may be '`S`' or '`D`'. The value '`S`' designates *non-summer* time. The value '`D`' designates *summer* (*daylight-saving*) time.

   **`HH`**: Hours offset from UTC/GMT in the interval [-12, +12]

   **`[0-59]`**: Minutes offset from UTC (in addition to hours offset) in the interval [0, 59] Default: **`0`**

   To set the zonetime to that of *Central Europe* or *Sweden*, invoke the command:

   **`clock timezone central-europe|sweden`**

   Example

   ```
   OS900(config)# clock timezone NAME E%sT -2 31
   Please login again following execution of this command.
   OS900(config)#
   ```

3. To set the *start* and *end* times for the summer, invoke the command:

   **`clock summer-time MONTH DAY <1993-2035> HH:MM MONTH DAY <1993-2035> HH:MM [OFFSET]`**

   where,

[72] UTC is a time scale that couples GMT, which is based solely on the Earth's varying rotation rate, with the time of highly accurate atomic clocks.

**MONTH**: (First appearance) Month in which summer *starts*. Any one of the following may be entered: **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, **dec**

**DAY**: (First appearance) Day in the month in which summer *starts*. Examples of valid entries are: **5**, **18**, **lastSun**, **lastMon**, **Sun>=8**, **Mon>=8**, **Sun<=7**, **Mon<=7**

where,

**lastSun**: Last Sunday in the month

**lastMon**: Last Monday in the month

**Sun>=8**: Earliest Sunday on or *after* the 8th of the month

**Mon>=8**: Earliest Monday on or *after* the 8th of the month

**Sun<=7**: Latest Sunday on or *before* the 7th of the month

**Mon<=7**: Latest Monday on or *before* the 7th of the month

**<1993-2035>**: (First appearance) Year in which summer *starts* in the interval [1993, 2035]

**HH:MM**: (First appearance) Time-of-day at which summer *starts*

**MONTH**: (Second appearance) Month in which summer *ends*. Any one of the following may be entered: **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, **dec**

**DAY**: (Second appearance) Day in the month in which summer *ends*. Examples of valid entries are: **5**, **18**, **lastSun**, **lastMon**, **Sun>=8**, **Mon>=8**, **Sun<=7**, **Mon<=7**

where,

**lastSun**: Last Sunday in the month

**lastMon**: Last Monday in the month

**Sun>=8**: Earliest Sunday on or *after* the 8th of the month

**Mon>=8**: Earliest Monday on or *after* the 8th of the month

**Sun<=7**: Latest Sunday on or *before* the 7th of the month

**Mon<=7**: Latest Monday on or *before* the 7th of the month

**<1993-2035>**: (Second appearance) Year in which summer *ends* in the interval [1993, 2035]

**HH:MM**: (Second appearance) Time-of-day at which summer *ends*

**[OFFSET]**: The forward offset (in the format HH:MM) to add to the time-of-day at which summer *starts*, i.e., to **HH:MM**. Default: 01:00

Example

```
OS900(config)# clock summer-time mar 17 2009 23:30 sep 4 2010 23:30 01:30
Please login again following execution of this command.
OS900(config)#
```

4. Get the Zonetime and summertime information by invoking the command:
   **clock timezone ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]**

   where,

   **clock**: Clock

   **timezone**: Time zone.

   **ftp**: FTP.

   **FTP-SERVER**: IP address or DNS name of the zonetime FTP server.

   **REMOTE-DIR**: Name of the directory containing the file that contains the zone information.

   **REMOTE-FILENAME**: Name of the file containing the zone information.

   **[USERNAME]**: (optional) Username that will be requested when attempting to access the NTP server on reentry to **configure terminal** mode.

   **[PASSWORD]**: (optional) Password that will be requested when attempting to access the NTP server on reentry to **configure terminal** mode.

As a result, a binary file with filename ***localtime*** is created containing zonetime and summertime information. The file is located in the directory **/etc**.

Example

```
OS900(config)# clock timezone ftp 10.90.136.190 ./File Tiger MyPassWord
OS900(config)#
```

5. Enter **ntp** mode.
6. Set the OS900 to operate in either of the following modes:

Client Mode

In this mode, the OS900 can be synchronized to the remote NTP server *but not* vice versa. To set the OS900 to operate in *client* mode with a remote NTP server, invoke the command:

**server IPADDR [key KEYNUM] [version VERNUM] [prefer]**

where,

**IPADDR**: IP address of the remote NTP server that is to provide UT timestamps to the OS900.

**key**: Authentication key.

**KEYNUM**: Code number with which authentication fields of each packet sent to a remote NTP server are to be encrypted. (This number must match the code number configured on the NTP server.)

**version**: NTP version.

**VERNUM**: NTP Version number to be used with outgoing NTP packets. Valid numbers are 1 to 3.

**prefer**: Mark the remote NTP server as the preferred source.

Below is an example showing the administrator inputs (in **bold**) for obtaining a UT timestamp.

```
OS900(config-ntp)# server 10.90.136.183 key 213213587 version 3 prefer
OS900(config-ntp)#
```

Peer Mode

In this mode, the OS900 can be synchronized to the NTP server *or* vice versa. The OS900 operates in symmetric active mode with the remote NTP server. To set the OS900 to operate in *peer* mode with a remote NTP server, invoke the command:

**peer IPADDR [key KEYNUM] [version VERNUM] [prefer]**

where,

**IPADDR**: IP address of the remote NTP server that is to provide UT timestamps to the OS900 or vice versa.

**key**: Authentication key.

**KEYNUM**: Code number with which authentication fields of each packet sent to a remote NTP server are to be encrypted. (This number must match the code number configured on the NTP server.)

**version**: NTP version.

**VERNUM**: NTP Version number to be used with outgoing NTP packets. Valid numbers are 1 to 3.

**prefer**: Mark the remote NTP server as the preferred source.

7. (Optional) Include additional remote NTP servers by repeating step *6*, above.
8. (Optional) Enable the NTP authentication feature of the OS900 by invoking the command:

   **authenticate**
9. (Optional) Define an authentication key by invoking the command:

   **authentication-key KEYNUM md5 KEYVALUE**

   where,

**KEYNUM**: Code number for accessing the remote NTP server in order to synchronize with it. (This number must match the code number configured on the remote NTP server.)

**md5**: Message Digest 5 encryption code/algorithm.

**KEYVALUE**: Authentication key value.

10. (Optional) Specify an encryption key that is trusted for the purpose of authenticating peers suitable for synchronization by invoking the command:

    **trusted-key KEYNUM**

    where,

    **KEYNUM**: Code number to be used with the NTP ***xntpc*** query/control program that diagnoses and fixes problems that affect the ***xntpd*** daemon operation. (This number must match the code number configured on the remote NTP server.)

11. Run NTP by invoking the command:

    **enable**

# Viewing

## NTP Status

To view the status of the NTP on the OS900, invoke the command:

**show ntp status**

There are three possible statuses:

1. ntp status = disable. This means that NTP is not running.
2. ntp status = enable but not running. This means that the OS900 cannot access the NTP server. In such case, there is no need to re-invoke the command **enable** (in step *11*, above) since the OS900 will attempt to connect to the NTP server about once every minute.
3. ntp status = enable and running. This means that the OS900 cannot access the NTP server and NTP is running.

Below, are three examples, one for each status. The line applicable to the status is marked red.

Example 1

```
OS900(config-ntp)# show ntp status                The answer may take some seconds.
NTP STATUS:
SERVERS:
                 server=10.90.136.183
PEERS:
                 peers are not defined
BROADCAST SERVER:
                 broadcast is disable
BROADCAST CLIENT:
                 broadcast client is disable
AUTHENTICATE:
                 authentication parameters are not defined
MISCELANIOUS:
                 broadcast delay is not defined
NTP ACTIVE MODE:
                 ntp status = disable
OS900(config-ntp)#
```

Example 2

```
OS900(config-ntp)# show ntp status
                 The answer may take some seconds.
NTP STATUS:
SERVERS:
                 server=10.90.136.254
PEERS:
                 peers are not defined
```

```
BROADCAST SERVER:
                 broadcast is disable
BROADCAST CLIENT:
                 broadcast client is disable
AUTHENTICATE:
                 authentication parameters are not defined
MISCELANIOUS:
                 broadcast delay is not defined
NTP ACTIVE MODE:
                 ntp status = enable but not running
                 (no defined servers are accessible).
OS900(config-ntp)#
```

Example 3

```
OS900(config-ntp)# show ntp status                 The answer may take some seconds.
NTP STATUS:
SERVERS:
                 server=10.90.136.183
PEERS:
                 peers are not defined
BROADCAST SERVER:
                 broadcast is disable
BROADCAST CLIENT:
                 broadcast client is disable
AUTHENTICATE:
                 authentication parameters are not defined
MISCELANIOUS:
                 broadcast delay is not defined
NTP ACTIVE MODE:
                 ntp status = enable and running.
OS900(config-ntp)#
```

## NTP Associations

To view the NTP associations, invoke the command:

**`show ntp associations`**

If the OS900 cannot access an NTP server, the message `ntpq: read: Connection refused` is displayed.

If the OS900 is connected to an NTP server, the NTP associations are displayed.

Example

```
OS900(config-ntp)# show ntp associations
 remote          refid          st t  when  poll  reach  delay  offset   jitter
===============================================================================
 10.90.136.183  128.139.6.30   2 u   7     64     7     0.634  385.097  37.608
OS900(config-ntp)#
```

NTP associations are displayed with variables and indicators, as shown in the example above.

### Variables

**`remote`** (peer)– IP address of peer.

**`refid`** (reference clock) – IP address of the server from which the NTP server obtained its timestamp (for the OS900).

**`st`** (Peer's stratum) – The downstream order of the peer. The stratum of the primary peer (source) is 1. Accordingly, if a peer stratum is 2, it means that it receives directly from the primary peer. If a peer stratum is 3, it means that it receives from the peer whose stratum is 2.

**`t`** – Time scale. (The value **`u`** designates UTC scale)

**`when`** – Time since last NTP packet received from peer.

**`poll`** – Polling interval (seconds)

**`reach`** – Peer reachability (bit string, octal)

**delay** – Round-trip delay to peer (milliseconds)
**offset** – Relative time of peer's clock to local time (milliseconds)
**jitter** – Short-time variation in frequency with components greater than 10 Hz

**Indicators**

Following are indicators and a

***** (if present) – Synchronized to this peer (NTP server).
**#** (if present) – Almost synchronized to this peer.
**+** (if present) – Peer selected for possible synchronization.
**-** (if present) – Peer is a candidate for selection.
**~** (if present) – Peer is statically configured.

## Time and Date

To display the *time*, invoke the command: **show time** (or **do show time** if not in **enable** mode).

Example

```
OS900# show time
Thu Dec 18 09:38:05 GMT 2008
OS900#
```

To display the *date*, invoke the command: **show date** (or **do show date** if not in **enable** mode).

Example

```
OS900# show date
Thu Dec 18 09:39:13 GMT 2008
OS900#
```

# Chapter 34: Network Address Translation (NAT)

## Definition

Network Address Translation (NAT) is a function that replaces an IP address and/or port ID in a packet with another IP address and/or port ID when the packet crosses a specific network interface.

## Purpose

NAT is used to:

- Connect hosts with non-registered (non-globally routable) IP addresses
- Save on registered (globally routable) IP addresses
- Provide security (by making an organization appear from the outside as using an IP address space that is in fact different from what the organization is using internally)
- Improve administration (by partitioning local/private IP addresses into groups, each having just one registered IP address or by renumbering into CIDR blocks)

## Compliance

NAT complies with RFC 1631.

## Types

There are two *types* of NAT:

***Source NAT*** – One or more local (private) IP addresses are translated (mapped) into one global (public) IP address.

***Destination NAT*** – One global IP address is translated (mapped) into one or more local IP addresses.

## Modes

There are two *modes* of NAT:

***Inband*** – For this mode only inband ports are used. Additional processing is performed by software in the address translation process. As a result, the throughput rate is only one-third that of out-of-band mode.

***Out-of-band*** – For this mode the out-of-band port as well is used. Address translation is performed directly. As a result, the throughput rate is triple that of inband mode.

## Principles of Operation

*Figure 45*, page *550*, schematically describes the principles of operation of Source NAT (SNAT) and Destination NAT (DNAT).

### Source NAT

In SNAT, the source IP address and/or source port ID is replaced.

### Destination NAT

In DNAT, the destination IP address and/or destination port ID is replaced.

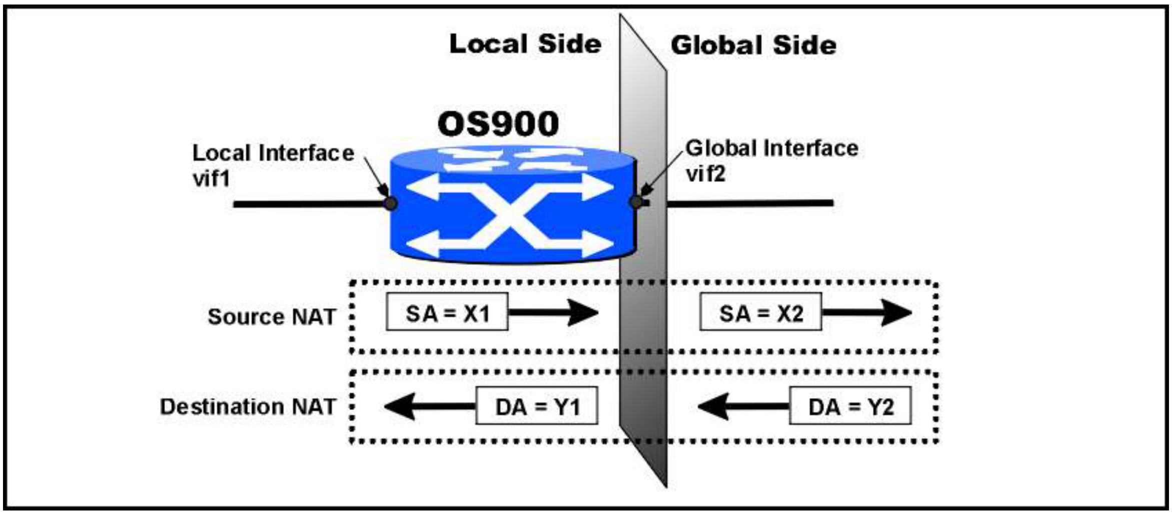



**Figure 45: NAT Operation**

# Data Paths

## Inband Mode

### Source NAT

Assuming that *Source* NAT has been activated, a packet from the *LAN* (local or private side) enters Local Interface. From the Local Interface it is sent to the CPU. The CPU translates the Local IP address into the appropriate Global IP address. The packet with the Global IP address is sent to the Global Interface and out to the WAN.

### Destination NAT

Assuming that *Destination* NAT has been activated, a packet from the *WAN* (global or public side) enters the Global Interface. From the Global Interface it is sent to the CPU. The CPU translates the Global IP address into the appropriate Local IP address. The packet with the Local IP address is sent to the Local Interface and in to the LAN.

## Out-of-band Mode

### Source NAT

Assuming that *Source* NAT has been activated, a packet from the *LAN* (local or private side) enters Local Port (Port 1 in the example). From the Local Port it is duplicated to the Co-Port[73] of the Out-of-band Port (Port 8 in the example), which is in the same VLAN as the Local Port. From Co-Port it is sent to the Out-of-Band Port and thereon to the CPU. The CPU translates the Local IP address into the appropriate Global IP address. The packet with the Global IP address is resent to the Out-of-Band Port and thereon to the Co-port. Using the ACL (which uses the direction of the packet to determine whether the packet is to be sent to the Local or Global VLAN), the Co-port selects the Global VLAN as the VLAN to which the packet belongs.

### Destination NAT

Assuming that *Destination* NAT has been activated, a packet from the *WAN* (global or public side) enters the Global Port (Port 2 in the example). From the Global Port it is duplicated to the Co-port of the Out-of-band Port (Port 8 in the example), which is in the same VLAN as that of the Global Port. From the Co-port it is sent to the Out-of-Band Port and thereon to the CPU. The CPU translates the Global IP address into the appropriate Local IP address. The packet with the Local IP address is resent to the Out-of-Band Port and thereon to the Co-port. Using the ACL (which uses the direction of the packet to determine whether the packet is to be sent to the Local or Global VLAN), the Co-port selects the local VLAN as the VLAN to which the packet belongs.

[73] The Co-port of an Out-of-band Port is a physical network port of the OS900 that is directly connected (with a patch cable) to the out-of-band port. The out-of-band port is marked ***MGT ETH*** on the front panel of the OS900.

# Implementation

## General

If the number of Local and Global IP addresses are different (e.g., several Local IP addresses and one Global IP address) NAT as well as Layer 4 port translation is performed.

NAT can be implemented to function in either of the following modes:

- Inband Mode
- Out-of-band Mode

## Inband Mode

### Source NAT

To implement Source NAT in inband mode:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

**`ip nat local IPV4_ADDR global IPV4_ADDR`**

where,

**`IPV4_ADDR`** (first appearance): IP address & mask of the *local* (private) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

**`IPV4_ADDR`** (second appearance): IP address & mask of the *global* (public) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

Example

***Required***: The Local (Private) network IP address is **10.80.80.0/24** and is to be represented in the Global (Public) network (e.g., Internet) by the IP address **192.168.2.1**.

***Solution***: Invoke the following Source NAT command:

**`ip nat local 10.80.80.0/24 global 192.168.2.1/32`**

where,

**`10.80.80.0/24`**: Local network IP address range

**`192.168.2.1/32`**: Global IP address representing it

### Destination NAT

To implement Destination NAT in inband mode:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

**`ip nat global IPV4_ADDR local IPV4_ADDR`**

where,

**`IPV4_ADDR`** (first appearance): IP address & mask of the *global* (public) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

**`IPV4_ADDR`** (second appearance): IP address & mask of the *local* (private) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

Example

***Required***: To permit Public (Internet) access to a server (e.g., TELNET server) in the local network using NAT. The local network IP address of the Server is **10.80.80.1** and the Internet IP address used for the access is **192.168.2.1**.

***Solution***: Invoke the following Destination NAT command:

**`ip nat global 192.168.2.1/32 local 10.80.80.1/32`**

where:

**`192.168.2.1/32`**: Public IP address of the server

`10.80.80.1/32`: Local IP address of the server

## Out-of-band Mode

To implement Source or Destination NAT in *out-of-band mode*:

1. Interconnect the out-of-band Management Port (***MGT ETH***) of the OS900 and a network port (e.g., Port 8) with an Ethernet Straight-wired patch cable (*Figure 78,* page *805*) or Cross-wired patch cable (*Figure 79,* page *805*). (This network port will be referred to as the Co-port.)
2. Create a 'Local' VLAN interface as follows:
   2.1. Include the Co-port and a network port that will serve as the *Local* Port (e.g., Port 1).
   2.2. Define a tag for the VLAN interface (e.g., Tag 10).
3. Create a 'Global' VLAN interface as follows:
   3.1. Include the Co-port and a network port that will serve as the *Global* Port (e.g., Port 2).
   3.2. Define a tag for the VLAN interface (e.g., Tag 20).
4. In the out-of-band Ethernet interface mode (entered by invoking the command **`interface out-of-band eth0`**):
   4.1. Enter the Destination IP address of the packets to be sent to the *Local* Port.
   4.2. Enter the Destination IP address of the packets to be sent to the *Global* Port.
5. Create an ACL that will enable the Co-port to direct an ingress packet to the *Local* Port or according to the Destination IP address as follows:
   5.1. To forward *IP* packets, create a rule that specifies the:
      5.1.1. Destination IP address of the packet to be forwarded to the *Local* Port using the command:
         **`dest-ip eq DEST_IP`**
      5.1.2. Action that swaps the VLAN Tag of the packet to that of the Local VLAN interface using the command:
         **`action tag swap TAG`**
   5.2. To forward *ARP* packets, create a rule that specifies the:
      5.2.1. Destination IP address of the packet to be forwarded to the *Local* Port using the command:
         **`dest-ip eq DEST_IP`**
      5.2.2. Packet *ethertype* after the VLAN header using the command:
         **`ethertype eq ETHERTYPE`**
      5.2.3. Action that swaps the VLAN Tag of the packet to that of the Local VLAN interface using the command:
         **`action tag swap TAG`**
   5.3. To forward *IP* packets, create a rule that specifies the:
      5.3.1. Destination IP address of the packet to be forwarded to the *Global* Port using the command:
         **`dest-ip eq DEST_IP`**
      5.3.2. Action that swaps the VLAN Tag of the packet to that of the Global VLAN interface using the command:
         **`action tag swap TAG`**
   5.4. To forward *ARP* packets, create a rule that specifies the:
      5.4.1. Destination IP address of the packet to be forwarded to the *Global* Port using the command:
         **`dest-ip eq DEST_IP`**
      5.4.2. Packet *ethertype* after the VLAN header using the command:
         **`ethertype eq ETHERTYPE`**

5.4.3. Action that swaps the VLAN Tag of the packet to that of the Global VLAN interface using the command:

**`action tag swap TAG`**

6. Bind the ACL to the Co-port using the command:

   **`port acl-binding-mode by-port CO-PORT`**

7. Activate the ACL at the Co-port using the command:

   **`port access-group ACL CO-PORT`**

8. The out-of-band management port (***MGT ETH***) can operate only with untagged packets. Since the Co-port is directly connected to the out-of-band management port, it to can operate only with untagged packets. As a result, the Co-port normally can be a member of only one VLAN. To enable the Co-port to be a member of two (or more) VLANs, invoke the command:

   **`port untagged-multi-vlans CO-PORT`**

9. To implement *Source* NAT (in out-of-band mode), invoke the command:

   **`ip nat local IPV4_ADDR global IPV4_ADDR`**

   where,

   **`IPV4_ADDR`** (first appearance): IP address & mask of the *local* (private) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

   **`IPV4_ADDR`** (second appearance): IP address & mask of the *global* (public) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

10. To implement *Destination* NAT (in out-of-band mode), invoke the command:

   **`ip nat global IPV4_ADDR local IPV4_ADDR`**

   where,

   **`IPV4_ADDR`** (first appearance): IP address & mask of the *global* (public) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

   **`IPV4_ADDR`** (second appearance): IP address & mask of the *local* (private) interface in the format **`a.b.c.d`**[**`/mask`**]. The mask can be up to 31 bits long.

Example

```
OS910(config)# write terminal

Building configuration...

Current configuration:

! version 2-0-3

interface vlan vif10
 tag 10
 ports 1,8
!
interface vlan vif20
 tag 20
 ports 2,8
!
interface out-of-band eth0
 ip 11.1.0.1/24
 ip 10.90.136.192/24
!
!
access-list extended acl1
 rule 10
  action tag swap 10
  dest-ip eq 11.1.0.0/24
```

```
 rule 20
  action tag swap 10
  ethertype eq 0x806
  dest-ip eq 11.1.0.0/24
 rule 30
  action tag swap 20
  dest-ip eq 10.90.136.0/24
 rule 40
  action tag swap 20
  ethertype eq 0x806
  dest-ip eq 10.90.136.0/24
!
port acl-binding-mode by-port 8
port access-group acl1 8
port untagged-multi-vlans 8
!
ip nat local 11.1.0.10/24 global 10.90.136.192/32
!
ip nat global 10.90.136.207/32 local 11.1.0.10/32
!
```

# Chapter 35: IGMP IP Multicast

## Terminology

***General Query:*** Message sent by an OS900 to learn which groups have members on an attached network.

***Group-specific Query:*** Message sent by an OS900 to learn if a particular group has members on an attached network.

***Membership Report:*** Message sent by a client (e.g., switch):

Requesting to join a multicast group, or

In response to a query (general or group-specific).

***Leave:*** Message sent when a client attempts to terminate the service provided.

***Querier Port State:*** The capability of an OS900 port to assume either of the following values:

Querier Port – Sends queries.

Non-Querier Port – Does not send queries.

A value of a querier port state can be changed in dynamic mode (default mode) or static mode.

In dynamic mode, the value is assigned to the querier port state according to the rules stated in RFC 2236. In this mode, the default value of querier port state is Querier Port.

In static mode, the value is assigned to the querier port state by the user with the aid of a CLI command.

***Server Port State:*** The capability of an OS900 port to assume either of the following values:

Server Port – Sends membership reports.

Non-Server Port – Does not send membership reports.

A value of a server port state can be changed in dynamic mode (default mode) or static mode.

In dynamic mode, the value assigned to the Server Port state depends on the:

1) Result of the comparison between the OS900's IP address and its neighbor.
2) Value of the querier port state (Querier Port or Non-Querier Port) of the OS900 port.

In this mode, the default value of server port state is Non-Server Port.

In static mode, the value is assigned to the server port state by the user with the aid of a CLI command.

## Definition

IGMP IP Multicast is the direction of selective IP multicast traffic (data, video, voice, etc.) to ports belonging to a particular IP Multicast group.

## Compliance

IGMP IP Multicast implementation in the OS900 complies IGMPv2 (IETC RFC 2236).

## Purpose

IGMP IP Multicast has the following purposes:

- **Selective Homing**: Direction of selective IP traffic to intended clients only!
  This has the following two advantages over the *broadcast* mode:

  - IP traffic does not reach unintended clients. This is useful in respect to discretion, billing, security, etc.
  - It does not load ports that are not required to receive the IP traffic.
- **Minimal Loading**: Forwarding of only a *single* copy of the IP traffic over the network! This has the following advantage over *unicast* mode: It does not send multiple copies of the IP traffic over the network to multiple clients belonging to the same multicast group; just one copy. This considerably reduces traffic load on the network. Thus a network could continue to function properly even for a large number of such groups.

# Applications

IP Multicast provides the most network bandwidth efficient means of source-to-destination trafficking in one-to-many and many-to-many applications, such as for example Multimedia (streaming media, remote education, audio/video conferencing, etc.)

*Figure 46* is an example of an application of IP Multicast.

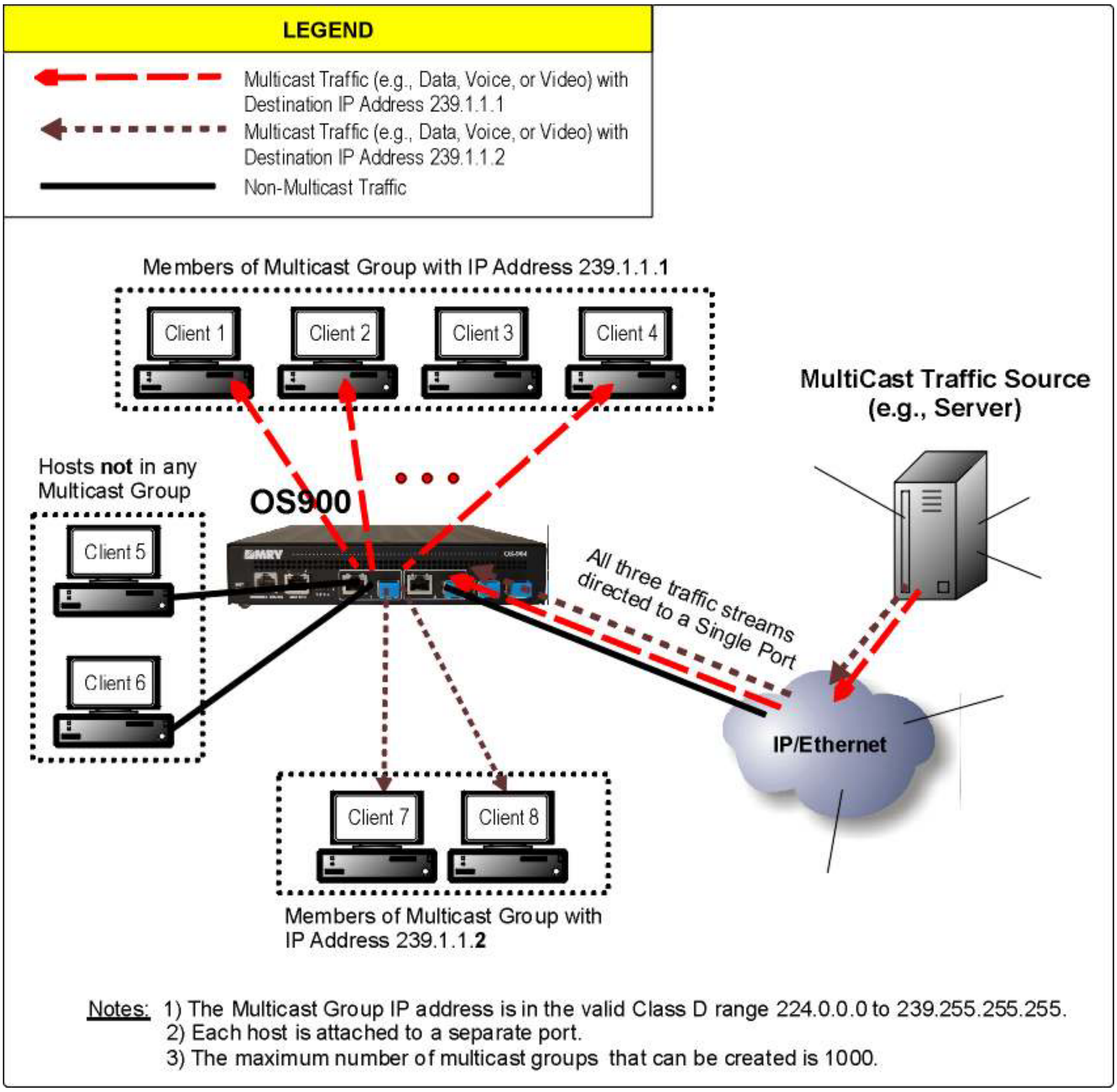



**Figure 46: IGMP IP Multicast Application Example**

# Functions

The OS900 uses the IGMP Snooping and Proxy functions for IP multicast. IGMPv2 is superior to IGMPv1 because it allows termination of group membership to be immediately reported by the

IGMP protocol. This capability is important for large-bandwidth multicast groups and subnets with highly volatile group membership.

**IGMP Snooping:** The OS900 uses the IGMP Snooping function to examine IGMP packets (e.g., query and report) to learn dynamically about multicast group membership and to make forwarding decisions accordingly. The OS900 features a new level of efficient IP Multicast support by examining all IGMP traffic in hardware at wire speed, and eliminating unwanted data streams so that they cannot impact network or endstation performance.

**IGMP Proxy:** The IGMP proxy function is used by the OS900 to identify members of a multicast group on a per-port basis, send ‘query’ messages, and sense ‘report’ (join) and ‘leave’ messages by which clients can join and leave multicast groups. IGMP Proxy has the functionality of IGMP querier interfaces (ports) as well as client interfaces. IGMP Proxy performs the router part of the IGMP protocol on its client interfaces, and the client part of the IGMP protocol on its querier interface. On receiving IP multicast data on a querier or client interface, the OS900 forwards the data only to client interfaces that are members of the specific multicast group. The OS900 forwards IGMP ‘report’ and ‘leave’ messages received from client interfaces to the querier interfaces.

# Principle of Operation

## Port States

The setting of states to OS900 ports by IGMP (when all the ports of OS900 **A** and OS900 **B** are set in dynamic mode) is described with the aid of the sample network in *Figure 47*, below. This network was chosen for its simplicity in order to facilitate explanation of the state setting principle.

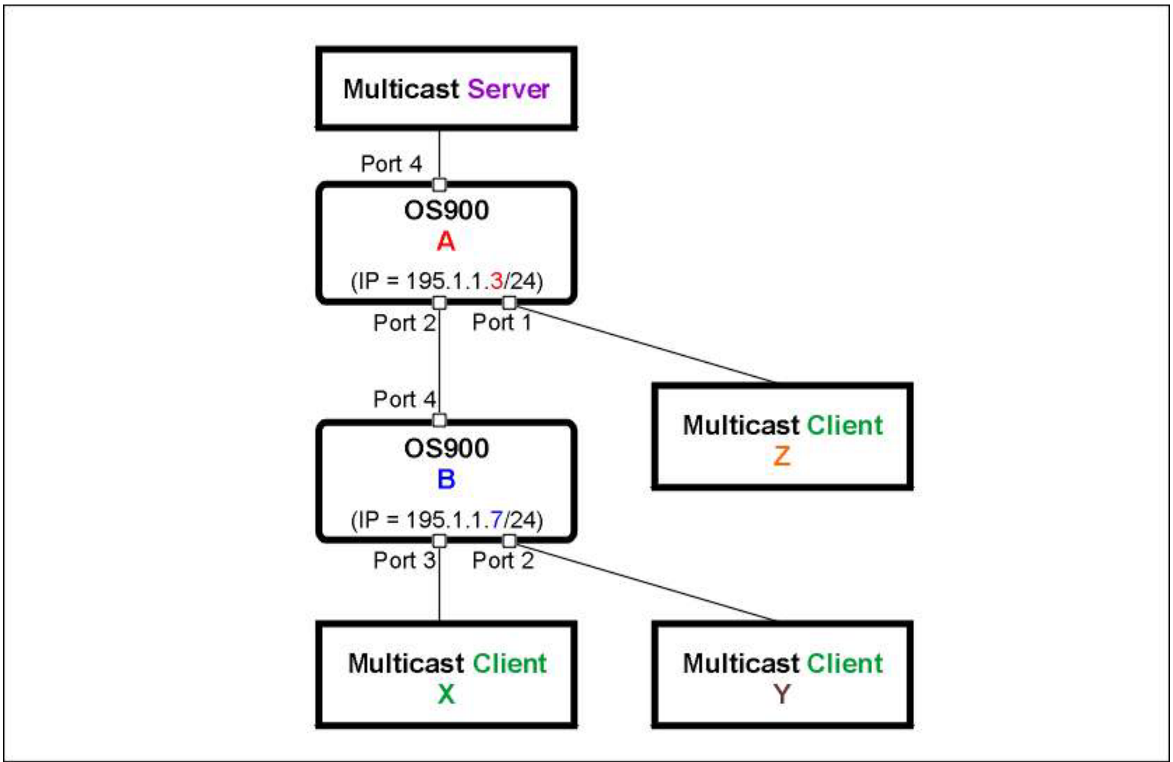



**Figure 47: IGMP IP Multicast Principle-of-Operation Network Example**

### Query

When IGMP is enabled, all the ports of the OS900 are initially set as querier ports. When a neighbor OS900 receives a query from any of these ports, the neighbor compares the IP address in the query with its own. If its own IP address is *lower*, the port at which it received the query remains as a querier port. If its own IP address is *higher*, the port at which it received the query becomes a non-querier port, i.e., it will not send query packets. According to *Figure 47*, Port 4 remains a querier port because the Multicast Server does not send queries and therefore IP addresses are not compared. When Port 2 receives a query from Port 4 it remains as a querier port because the IP address of OS900 **A** is lower than the IP address of OS900 **B**. When Port 4 receives a query from Port 2 it changes its state from a querier port into a non-querier port because the IP address of OS900 **B** is higher than the IP address of OS900 **A**. Since ports 1, 2, and 3 are connected to clients, they will not receive queries and, therefore, will continue to remain as querier ports.

### Server

When IGMP is enabled, all the ports of the OS900 are initially set as Non-Server Ports.

In dynamic mode, when a port whose 'server port state' is:

– Non-Server Port changes its 'querier port state' from Querier Port to Non-Querier Port, the port will change its 'server port state' from Non-Server Port to Server Port.

– Server Port changes its 'querier port state' from Non-Querier Port to Querier Port, the port will change its 'server port state' from Server Port to Non-Server Port.

According to *Figure 47*, when Port 4 (after it has changed to Non-Querier Port) receives a query from Port 2, it changes its 'server port state' to Server Port.

Summary:

Ports that transmit queries in the direction of multicast clients will become querier ports. Ports that respond to a query with a report message sent in the direction of multicast servers will become server ports.

For *Figure 47*, Ports 1, 2, and 3 become querier ports; Port 4 becomes a server port.

## Leave Modes

The OS900 can be configured to respond to a client requesting to leave a multicast group in either of the following modes:

– Regular (per the standard)

– Fast

### Regular

In regular leave mode, when an OS900 receives a 'leave' message from a client, it sends a ''group-specific query' to the client and waits until the end of the standard response time. If no 'report' is received from this client during this wait, the specific client is removed from the multicast group. If a 'report' is received from this client during this wait, the client is retained in the multicast group.

This mode may delay a client by a few seconds from joining another multicast group.

### Fast

In fast leave mode (entered by invoking the command **`fast-leave`**, described in the section *Selecting Fast Leave Mode*, page *563*),, unlike in regular leave mode, a client can switch to another multicast group immediately. The OS900 removes the specific client immediately and then sends the 'group-specific query afterward. Fast leave mode is the default mode.

### Special

In special mode (entered by invoking the command **`no query-specific`**, described in the section *Special Mode*, page *561*), when the OS900 receives a 'leave' message it removes the specific client immediately without sending a group-specific query.

# Rules

1. If dynamic mode (i.e., IGMP mode of registration) is selected for 'querier port state' and 'server port state', mediation devices (e.g., OS900s) in any path from a multicast server to a multicast client must have progressively higher IP addresses.

2. In *static* mode:
   – Ports that are to direct traffic to multicast clients must be configured as query and non-server ports.
   – Ports that are to direct reports to servers must be configured as server and non-querier ports.

   IGMP does this automatically in *dynamic* mode (default mode) of the OS900.
3. For each port, either both ‘querier port state’ and ‘server port state’ must be set to dynamic mode or both must be set to static state.
4. If IGMP is disabled (using the command **`no enable`** in **`igmp`** mode), static multicast entries can be viewed using the command **`write terminal`** or **`show running-config`** in **`enable`** mode.
5. The multicast group IP address must be in the range 224.0.0.0 to 239.255.255.255.
6. To distinguish between two multicast groups, their two IP addresses must differ from each other in their 23 LSBs.
7. A static multicast group can be created (using the command **`mc-group address`**) if all of the following conditions are met:
   – An interface with a tag matching the tag of the multicast group (to be created) exists.
   – An IP address is assigned to this interface.
   – IGMP is enabled on this interface.
8. A single or a range of multicast groups is automatically deleted if any of the following occurs:
   – An interface with a tag matching the tag of the multicast group created (using the command **`mc-group address`**) is deleted.
   – The IP address of the interface is deleted.
   – IGMP is disabled on the interface
9. Multicast groups must not overlap.
10. For a client *to be able* to receive traffic addressed to a multicast group, the client needs to use an IP multicast support application that implements IGMP on networks that support IGMP. (Such networks effectively eliminate multicast traffic on segments that are not destined to receive this traffic.)
11. For a client to receive traffic addressed to a multicast group, it must be a member of the group.
12. Traffic is sent to clients that joined the multicast group so long as there is at least one member that has not requested to leave the group.

# Usage

## Entering IGMP Mode

To *enter* the mode in which the OS900 can be configured for IGMP multicast operation:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`igmp`**.

Example

```
MRV OptiSwitch 910 version d0733-08-01-06
OS900 login: admin
Password: ******

OS900> enable
OS900# configure terminal
OS900(config)# igmp
```

```
OS900(config-igmp)#
```

## Enabling IGMP Multicast

To *enable* IGMP Multicast:

1. Enter **igmp** mode.
2. Invoke the command:

   **enable**

Example

```
OS900# configure terminal
OS900(config)# igmp
OS900(config-igmp)# enable
OS900(config-igmp)#
```

## Disabling IGMP Multicast

By default, IGMP Multicast is disabled (for all VLAN interfaces).

To *disable* IGMP Multicast (for all VLAN interfaces):

1. Enter **igmp** mode.
2. Invoke the command:

   **no enable**.

Example

```
OS900# configure terminal
OS900(config)# igmp
OS900(config-igmp)# no enable
OS900(config-igmp)#
```

## Enabling IGMP Proxy

This is the default mode.

IGMP proxy includes snooping. In this mode, the OS900 collects information on the received IGMP packets (query, join, or leave) from a Multicast client and then sends a request on behalf of the members of the Multicast Group as initiator. The request is sent with the Source MAC address of the OS900 and Source IP address. The Source IP address is that of the OS900 VLAN Interface, via which the request is sent. If the VLAN Interface does not have an IP address, the Source IP address will be 0.0.0.0.

To *enable* IGMP proxy mode for the OS900:

1. Enter **igmp** mode.
2. Invoke the command:

   **mode igmp-proxy**

Example

```
OS900(config-igmp)# mode igmp-proxy
OS900(config-igmp)#
```

## IGMP Pure Snooping

### Enabling

To set the OS900 to forward Multicast Group IGMP packets passively (i.e., to send as many join requests as it receives from members of a Multicast Group), and to flood all the ports of the VLAN with these packets:

1. Enter **igmp** mode.
2. Invoke the command:

   **mode pure-snooping**

Example

```
OS900(config-igmp)# mode pure-snooping
OS900(config-igmp)#
```

### Disabling

This is the default state.

To disable IGMP pure snooping (i.e., to disable forwarding of Multicast Group IGMP packets passively as well as flooding of all the ports of the VLAN with these packets, and to enable IGMP proxy mode):

1. Enter **igmp** mode.
2. Invoke the command:
   **no mode pure-snooping**

Example

```
OS900(config-igmp)# no mode pure-snooping
OS900(config-igmp)#
```

## Query Flooding

### Enabling

To set the OS900 to act as IGMP proxy for join and leave packets and to flood all the ports of the VLAN with query packets:

1. Enter **igmp** mode.
2. Invoke the command:
   **mode query-flooding**

Example

```
OS900(config-igmp)# mode query-flooding
OS900(config-igmp)#
```

### Disabling

This is the default mode.

To disable flooding with query packets as well as proxy for non-query packets, and to enable IGMP proxy:

1. Enter **igmp** mode.
2. Invoke the command:
   **no mode query-flooding**

Example

```
OS900(config-igmp)# no mode query-flooding
OS900(config-igmp)#
```

## Special Mode

### Enabling

This mode is used when it is required to reduce traffic load on the CPU which can be considerably high when, for instance, many hosts in Multicast Groups send a 'leave' request concurrently.

To enable Special Mode, i.e., to prevent sending of Query Specific packets when a 'leave' request is received:

1. Enter **igmp** mode.
2. Invoke the command:
   **no query-specific**

Example

```
OS900(config-igmp)# no query-specific
OS900(config-igmp)#
```

**Disabling**

This is the default mode.

This mode is used when it is required to prevent disconnection of all hosts in a Multicast Group (connected, for example, via a hub) when ***not*** all hosts in the Multicast Group send a ‘leave’ request. The OS900 prevents disconnection by sending a Query Specific packet.

To disable Special Mode, i.e., to allow sending of Query Specific packets when a ‘leave’ request is received:

1. Enter **`igmp`** mode.
2. Invoke the command:
   **`query-specific`**

Example

```
OS900(config-igmp)# query-specific
OS900(config-igmp)#
```

**Default**

To revert to the default mode, i.e., to disable Special Mode, i.e., to allow sending of Query Specific packets when a ‘leave’ request is received:

1. Enter **`igmp`** mode.
2. Invoke the command:
   **`query-specific default`**

Example

```
OS900(config-igmp)# query-specific default
OS900(config-igmp)#
```

## Enabling IGMP Multicast for a VLAN Interface

To enable IGMP Multicast for a specific VLAN interface:

1. Enter the mode of the VLAN interface for which IGMP Multicast is to be enabled (as described in the section *Configuring*, page *181*).
2. Invoke the command:
   **`igmp-enable`**.

Example

```
OS900(config)# interface vif7
OS900(config-vif7)# igmp-enable
OS900(config-vif7)#
```

**Note**

The command **`igmp-enable`** can enable IGMP Multicast for a VLAN interface provided IGMP is globally enabled as described the section *IGMP Multicast*, page *560*.

## Disabling IGMP Multicast for a VLAN Interface

By default, IGMP Multicast is disabled for an VLAN interface.

To disable IGMP Multicast for a specific VLAN interface:

1. Enter the mode of the VLAN interface for which IGMP Multicast is to be disabled.
2. Invoke the command:
   **`no igmp-enable`**.

Example

```
OS900(config)# interface vif7
OS900(config-vif7)# no igmp-enable
OS900(config-vif7)#
```

## Changing Query Interval

The query interval is the wait period (in seconds) between queries sent by a querier.

By default, the query interval is 60 seconds.

To change the query interval:

1. Enter **igmp** mode.
2. Invoke the command:

   **query TIME**

   where,

   **TIME** = Query interval in seconds; a number selectable from the range **30** to **6000**.

Example

```
OS900(config)# igmp
OS900(config-igmp)# query 285
OS900(config-igmp)#
```

## Changing Aging Time

Aging time is the time the OS900 will wait for a ‘report’ from a multicast client before it removes membership of the client port from the multicast group.

By default, the aging time for any multicast group is 60 seconds.

To change the current aging time:

1. Enter **igmp** mode.
2. Invoke the command:

   **aging TIME**.

   where,

   **TIME** = Aging time (in seconds). Valid values are in the range 30 to 6000.

Example

```
OS900# configure terminal
OS900(config)# igmp
OS900(config-igmp)# aging 120
OS900(config-igmp)#
```

## Selecting Fast Leave Mode

Fast leave mode of the OS900 enables a client to delete a multicast group immediately. By default, the OS900 operates in fast leave mode.

To select fast leave mode:

1. Enter **igmp** mode.
2. Invoke the command:

   **fast-leave**

Example

```
OS900(config)# igmp
OS900(config-igmp)# fast-leave
OS900(config-igmp)#
```

## Selecting Regular Leave Mode

Regular leave mode is complaint to IETC RFC 2236 standard. It forces a client attempting to ‘leave’ a multicast group to wait until the end of the standard response time.

When an OS900 receives a ‘leave’ message, it sends a group-specific query to determine whether the ‘leave’ message can be ignored.

To set fast leave mode:

1. Enter **igmp** mode.
2. Invoke the command:

   **no fast-leave**

Example

```
OS900(config)# igmp
OS900(config-igmp)# no fast-leave
OS900(config-igmp)#
```

## Creating Static Multicast Group(s)

The maximum number of multicast groups that can be created is 1000.

Multicast groups must not overlap.

To distinguish between two multicast groups, their two IP addresses must differ from each other in their 23 LSBs.

A multicast group can be created if all of the following conditions are met:

- A VLAN interface with a tag matching the tag of the multicast group (to be created) exists. (Configuration of VLAN interfaces is described in ***Chapter 7:*** *Interfaces*, in the section *Configuring*, page *181*.)
- An IP address is assigned to this interface. (Assignment of an IP address to a VLAN interface is described in ***Chapter 7:*** *Interfaces*, in the section *Configuring*, page *181*.)
- IGMP is enabled on this interface using the **igmp-enable** command as described in the section *Enabling IGMP Multicast for a VLAN Interface*, page *562*.

### Single

To create a *single* static multicast group:

1. Enter **igmp** mode.
2. Invoke the command:

   **mc-group address GROUP-IP tag TAG ports PORTS-GROUP**.

   where,

   **GROUP-IP** = IP address of multicast group. Valid IP addresses are in the range 224.0.0.0 to 239.255.255.255. (The range 224.0.0.0 to 224.0.0.255 is reserved by IANA for use by network protocols on a local network segment. Packets with an IP address in this range are local in scope and are not forwarded by IP routers. As a result, the packets will not leave the local network.)

   **TAG** = Tag of the interface containing the ports to be members of the multicast group.

   **PORTS-GROUP** = Group of ports to be members of the multicast group.

Example

```
OS900(config)# igmp
OS900(config-igmp)# mc-group address 224.1.1.5 tag 300 ports 1,2
Number of multicast groups is 1.
OS900(config-igmp)#
```

### Multiple

To create *multiple* static multicast groups:

1. Enter **igmp** mode.
2. Invoke the command:

   **mc-group address FIRST-GROUP-IP last-address LAST-GROUP-IP tag TAG ports PORTS-GROUP**

   where,

   **FIRST-GROUP-IP** = Lowest IP address in the sequence of IP addresses to be assigned to the multicast groups. Valid IP addresses are in the range 224.0.0.0 to 239.255.255.255.

   **LAST-GROUP-IP** = Highest IP address in the sequence of IP addresses to be assigned to the multicast groups.

**TAG** = Tag of the interface containing the ports to be members of the multicast groups.

**PORTS-GROUP** = Group of ports to be members of the multicast groups.

Example

```
OS900(config)# igmp
OS900(config-igmp)# mc-group address 225.1.2.1 last-address 225.1.3.15 tag 10 ports 4
Number of multicast groups is 271.
OS900(config-igmp)#
```

## Deleting Static Multicast Group(s)

A single or a range of multicast groups is *automatically* deleted if any of the following occurs:

– An interface with a tag matching the tag of the multicast group created (using the command **mc-group address**) is deleted.
– The IP address of the interface is deleted.
– IGMP is disabled on the interface

### Single

To delete a *single* static multicast group:

1. Enter **igmp** mode.
2. Invoke the command:

**no mc-group address GROUP-IP tag TAG ports PORTS-GROUP**.

where,

**GROUP-IP** = IP address of multicast group.

**TAG** = Tag of the interface containing the ports that are members of the multicast group.

**PORTS-GROUP** = Group of ports that are members of the multicast group.

Example

```
OS900(config)# igmp
OS900(config-igmp)# no mc-group address 224.1.1.5 tag 300 ports 1,2
OS900(config-igmp)#
```

### Multiple

To delete *multiple* static multicast groups:

1. Enter **igmp** mode.
2. Invoke the command:

**no mc-group address FIRST-GROUP-IP last-address LAST-GROUP-IP tag TAG ports PORTS-GROUP**

where,

**FIRST-GROUP-IP** = Lowest IP address in the sequence of IP addresses assigned to the multicast groups.

**LAST-GROUP-IP** = Highest IP address in the sequence of IP addresses assigned to the multicast groups.

**TAG** = Tag of the interface containing the ports that are members of the multicast groups.

**PORTS-GROUP** = Group of ports that are members of the multicast groups.

Example

```
OS900(config)# igmp
OS900(config-igmp)# no mc-group address 225.1.2.1 last-address 225.1.3.15 tag 10 ports 4
OS900(config-igmp)#
```

## Setting Querier Port State in *Dynamic* Mode

In dynamic mode (default mode), a 'querier port state' can set to Non-Querier Port or Querier Port depending on the network topology.

To set dynamic 'querier port state' for *any* port:

1. Enter **igmp** mode.
2. Invoke the command:
   **port querier dynamic PORTS-GROUP|all**
   where,
   **PORTS-GROUP** = Group of ports to be set in dynamic 'querier port state'.
   **all** = All ports to be set in dynamic 'querier port state'.

The default value of 'querier port state' in dynamic mode is Querier Port.

Example

```
OS900(config)# igmp
OS900(config-igmp)# port querier dynamic 2-4
OS900(config-igmp)#
```

## Setting Server Port State in *Dynamic* Mode

In dynamic mode (default mode), a 'server port state' port can set to Non-Server Port or Server Port depending on the network topology.

To set dynamic 'server port state' for *any* port:

1. Enter **igmp** mode.
2. Invoke the command:
   **port server dynamic PORTS-GROUP|all**
   where,
   **PORTS-GROUP** = Group of ports to be set in dynamic 'server port state'.
   **all** = All ports to be set in dynamic 'server port state'.

The default value of 'server port state' in dynamic mode is Non-Server Port.

Example

```
OS900(config)# igmp
OS900(config-igmp)# port server dynamic 1-3
OS900(config-igmp)#
```

## Setting Querier Port State in *Static* Mode

'Querier port state' in static mode can be changed or freed to change only by the user.

'Querier port state' of a port may be changed from dynamic mode to static mode by setting either one of the following values to the port:

– Querier Port
– Non-Querier Port

### Querier Port

To set static 'Querier Port' to *a* port:

1. Enter **igmp** mode.
2. Invoke the command:
   **port querier static PORTS-GROUP|all**
   where,
   **PORTS-GROUP** = Group of ports to be set to static Querier Port.
   **all** = All ports to be set to static Querier Port.

Example

```
OS900(config)# igmp
OS900(config-igmp)# port querier static 2-4
OS900(config-igmp)#
```

#### Non-Querier Port

To set static 'Non-Querier Port' to *a* port:

1. Enter **igmp** mode.
2. Invoke the command:
   **port not-querier static PORTS-GROUP|all**
   where,
   **PORTS-GROUP** = Group of ports to be set to static Non-Querier Port.
   **all** = All ports to be set to static Non-Querier Port.

Example

```
OS900(config)# igmp
OS900(config-igmp)# port not-querier static 1,2
OS900(config-igmp)#
```

## Setting Server Port State in *Static* Mode

'Server port state' in static mode can be changed or freed to change only by the user.

'Server port state' of a port may be changed from dynamic mode to static mode by setting either one of the following values to the port:

– Server Port
– Non-Server Port

#### Server Port

To set static 'Server Port' to a port:

1. Enter **igmp** mode.
2. Invoke the command **port server static PORTS-GROUP|all**
   where,
   **PORTS-GROUP** = Group of ports to be set to static Server Port.
   **all** = All ports to be set to static Server Port.

Example

```
OS900(config)# igmp
OS900(config-igmp)# port server static 3,4
OS900(config-igmp)#
```

#### Non-Server Port

To set static Non-Server Port to a port:

1. Enter **igmp** mode.
2. Invoke the command:
   **port not-server static PORTS-GROUP|all**
   where,
   **PORTS-GROUP** = Group of ports to be set to static Non-Server Port.
   **all** = All ports to be set to static Non-Server Port.

Example

```
OS900(config)# igmp
OS900(config-igmp)# port not-server static 2-4
OS900(config-igmp)#
```

## Source IP Address

#### Defining

To define an IP address to be used as the Source IP Address (in the IP header) of IGMP-query (general and specific) packets, invoke the command:

1. Enter **igmp** mode.
2. Invoke the command:

**query-specific-ip A.B.C.D**

where,

**A.B.C.D** = IP address for the IGMP-query packets.

**Canceling**

To cancel use of the user-defined Source IP address in the IP header of IGMP-query packets:

1. Enter **igmp** mode.
2. Invoke the command:

   **no query-specific-ip**

## Forced Source IP Address

To cause IGMP packets to be transmitted from an Inband VLAN Interface with Source IP address 0.0.0.0:

1. Enter **igmp** mode.
2. Invoke the command

   **zero-source-ip**

To cancel use of 0.0.0.0 as Source IP address for IGMP packets, invoke the command: **no zero-source-ip**.

## Clearing Statistics

To clear IGMP statistics:

1. Enter **igmp** mode.
2. Invoke the command

   **clear igmp-statistics**

## Viewing IGMP Settings

To view the current IGMP settings:

1. Enter **igmp** mode.
2. Invoke the command:

   **show**

Example

```
 OS900(config-igmp)# show
fast leave              : Yes
query                   : 60 sec
aging                   : 180 sec
enable                  : No
source IP for IGMP msg  : Interface IP
src IP query-specific   : not defined
send Query Specific     : Yes
mode                    : IGMP proxy
OS900(config-igmp)#
```

## Viewing Port Modes and States

To view the current mode and state of a group of ports:

1. Enter **igmp** mode.
2. Invoke the command:

   **show igmp-port [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports about which IGMP information is to be displayed. (If no port number is entered for this argment, information about all the ports is displayed.)

Alternatively, the current mode and state of ports can be viewed by entering **`enable`** mode and invoking the command: **`show igmp igmp-port PORTS-GROUP`**.

Example

```
OS900(config-igmp)# show igmp-port 4

Ports  QUERIER         SERVER         ROUTER-IP      NUM-IGMP-VLANS
--------------------------------------------------------------------
 4     YES (dynamic)   NO  (dynamic)                 0

OS900(config-igmp)#
```

## Viewing Multicast Groups

### Single Entry

To view *settings* of one current IP multicast group:

1. Enter **`igmp`** mode.
2. Make sure that IGMP is enabled (using the command **`enable`**).
3. Invoke the command **`show mc-ip entry IP-ADDRESS`**.
   where,
   **`IP-ADDRESS`** = IP address of multicast group.

The headings of the entry (see example below) have following significance:

`Group-IP:` IP address of multicast group.

`num-Ifs:` Number of VLAN interfaces one or more of whose ports are members of the multicast group.

`Flags:` (Applies for *all* the VLAN interfaces.) Type*s* of registration in the multicast group*s*.
Possible types are:
`I` = IGMP-implemented registration
`S` = User-implemented registration
`SI` or `SI` means that there are ports that have been registered by IGMP and ports that have been registered by a user.

`Tag:` Tag of VLAN interface one or more of whose ports are in the multicast group.

`Vidx:` Index of multicast group.

`Flags:` (Applies for *specific* VLAN interfaces.) Type of registration in the multicast group.
Possible types are: `I` or `S`.

`num-Ports:` Number of ports (of the specific interface) that are members of the multicast group.

`PORTs:` ID of ports (of the specific interface) that are members of the multicast group.

Example

```
OS900(config)# igmp
OS900(config-igmp)# show mc-ip entry 225.1.1.1
Codes of the Flags: I - IGMP registration, S - Static registration.
   Group-IP     num-IFs Flags Tag  Vidx Flags num-Ports PORTs
-----------------------------------------------------------------
225.1.1.1         2       SI
                              10   4097  S    4         1-3
                              20   4098  I    1         4
OS900(config-igmp)#
```

(Alternately, the *settings* of one current IP multicast group can be viewed from **`enable`** mode by invoking the command: **`show igmp mc-ip entry A.B.C.D`**.)

### All Entries

To view settings of *all* current IP multicast groups:

1. Enter **`igmp`** mode.
2. Make sure that IGMP is enabled (using the command **`enable`**).
3. Invoke the command **`show mc-ip table`**.

Example

```
OS900(config-igmp)# show mc-ip table
Codes of the Flags: I - IGMP registration, S - Static registration.
   Group-IP     num-IFs Flags Tag  Vidx Flags num-Ports PORTs
--------------------------------------------------------------------
 225.1.1.1         3      I
                              50   4567 I     1         3
                              25   4844 I     1         1
                              16   4841 I     1         2
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
 225.1.1.2         2      I
                              50   4568 I     1         3
                              25   4845 I     1         1
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
 225.1.1.3         2      I
                              50   4569 I     1         3
                              25   4846 I     1         1
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
 225.1.1.4         2      I
                              50   4570 I     1         3
                              25   4847 I     1         1
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
 225.1.1.5         2      I
                              50   4571 I     1         3
                              25   4848 I     1         1
OS900(config-igmp)#
```

'`Group-IP`' designates multicast group.

'`Tag`' designates multicast interface ID.

(Alternately, the *settings* of *all* current IP multicast groups can be viewed from **`enable`** mode by invoking the command: **`show igmp mc-ip table`**.)

## Viewing Number of Multicast Groups and Entries

The number of multicast groups is the number of IP addresses assigned to all the multicast groups. This is the number of IP addresses under the heading '`Group-IP`' in the Multicast IP table shown in the example in section *All Entries*, page *569*. The number of multicast groups in the example is 5.

The number of multicast entries is the number of IP address assignments to all the multicast interfaces. The IDs of the multicast interfaces appear under the heading '`Tag`' in the Multicast IP table shown in the example in section *All Entries*, page *569*. The number of multicast entries in the example is 3 (for '`225.1.1.1`' due to tags 50, 25, and 16) + 1 (for '`225.1.1.2`' due to tags 50 and 25) + 1 (for '`225.1.1.3`' due to tags 50 and 25) +1 (for '`225.1.1.4`' due to tags 50 and 25) +1 (for '`225.1.1.5`' due to tags 50 and 25) = 11 (multicast entries). The maximum possible number of multicast entries is 1020.

To view the *number* of current IP multicast groups:

1. Enter **`igmp`** mode.
2. Make sure that IGMP is enabled (using the command **`enable`**).
3. Invoke the command:
   **`show mc-ip number`**

Example

```
OS900(config-igmp)# show mc-ip number
Numbers of SW-entries: 800, HW-entries: 1000
OS900(config-igmp)#
```

'`SW-entries`' designates multicast *groups*.

'`HW-entries`' designates multicast *entries*.

(Alternately, the number of IP addresses assigned to all the multicast groups can be viewed from **`enable`** mode by invoking the command: **`show igmp mc-ip number`**.)

### Viewing Multicast Entries

To view IGMP IP multicast entries assigned to client ports:

1. Enter **igmp** mode.
2. Invoke the command:

   **show mc-ip port PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports whose assigned IP multicast entries are to be viewed.

### Viewing Multicast Group in a VLAN

To view IGMP IP multicast group (forwarding entries) whose ports are in a specific VLAN:

1. Enter **igmp** mode.
2. Invoke the command:

   **show mc-ip vid TAG**

   where,

   **TAG**: Tag of VLAN one or more of whose ports are in the IGMP IP multicast group to be displayed.

(Alternately, the IP multicast entries assigned to an Inband VLAN Interface can be viewed from **enable** mode by invoking the command: **show igmp mc-ip vid TAG**.)

### Viewing Statistics

To view IGMP statistical information about ports:

1. Enter **igmp** mode.
2. Invoke the command:

   **show igmp-statistics [PORTS-GROUP]**

   where,

   **[PORTS-GROUP]**: Group of ports about which IGMP statistical information is to be displayed. (If no port number is entered for this argment, information about all the ports is displayed.)

Alternatively, IGMP statistical information about ports can be viewed by entering **enable** mode and invoking the command: **show igmp igmp-statistics [PORTS-GROUP]**.

## Configuration

### General

Setting of states to ports can be done in *dynamic* or *static* mode. In dynamic mode, IGMP sets the states automatically. In static mode, the user sets the states. The state set to a port in static mode can be changed or freed to change only by the user.

Dynamic mode has two advantages over static mode:

- It relieves the user of the burden of configuring each OS900 port individually in a network that could possibly have hundreds of ports.
- It automatically (and within a few seconds) accomplishes network convergence (recovery) when mediation devices (e.g., switches or routers) are added or removed from the network.

Dynamic mode is the default mode.

### Procedure

The detailed configuration procedure for an OS900 to operate in the IGMP multicast protocol is as follows:

1. Create a VLAN interface that has:
   a. Ports that are to be made members of a multicast group.

   b. A VLAN tag.
   c. An IP address.

   For details, refer to ***Chapter 7:*** *Interfaces*, page *177*.
2. Enable IGMP on the VLAN interface as described in the section *Enabling IGMP Multicast for a VLAN Interface*, page *562*.
3. Enable IGMP multicast as described in the section *Enabling IGMP Multicast*, page *560*.
4. If required, create a static multicast group containing ports to be members as described in the section *Creating Static Multicast Group(s)*, page *564*.
5. For each path from a server to a client, if an OS900 has an IP address lower than *any* upstream OS900 in the path, the following must be done:
   a. The port of its immediate upstream neighbor (to which it is connected) must be set to static ‘Query Port’ (as described in the section *Querier Port*, page *566*).
   b. Its own port must be set to static ‘Server Port’ (as described in the section *Server Port*, page *567*).
6. (Optional) Change the query interval as described in the section *Changing Query Interval*, *563*.
7. (Optional) Change the aging time as described in the section *Changing Aging Time*, page *563*.
8. (Optional) Change the ‘leave’ mode as described in the section *Leave Modes*, *558*.

## Example

Referring to *Figure 47*, page *557*, ‘server port state’ and ‘querier port state’ of the OS900 ports will be correctly set in dynamic mode by IGMP since the OS900s in any path from the multicast server to a multicast client have progressively higher IP addresses.

If, however, in a path from a multicast server to a multicast client there is an OS900 with an IP address lower than an upstream OS900 in the path, the setting by IGMP would be incorrect. *Figure 48*, below, shows OS900s with IP addresses that ***do not*** get progressively higher in all the paths from the multicast server to the multicast clients. For e.g., in the path to C4, C5, or C6, the IP address gets higher in going from OS900 **A** to OS900 **B** (which complies with IGMP) but gets lower in going from OS900 **B** to OS900 **C** (which conflicts with IGMP). Accordingly, IGMP will succeed in correctly configuring the ports for the paths from the multicast server to C1, C2, and C3. However, IGMP will fail to correctly configure the ports for the paths to C4, C5, and C6. Specifically, Port 3 will set to Non-Query Port (although it is required to set to Query Port) because the IP address of OS900 **B** is higher than that of OS900 **C**. Port 1 will set to Query Port and Non-Server Port (although it is required to set to Server Port).

To resolve this problem, Port 3 and Port 1 have to be set *statically*. Port 3 must be set using the procedure described in the section *Querier Port*, page *566*. Port 1 must be set using the procedure described in the section *Server Port*, page *567*.

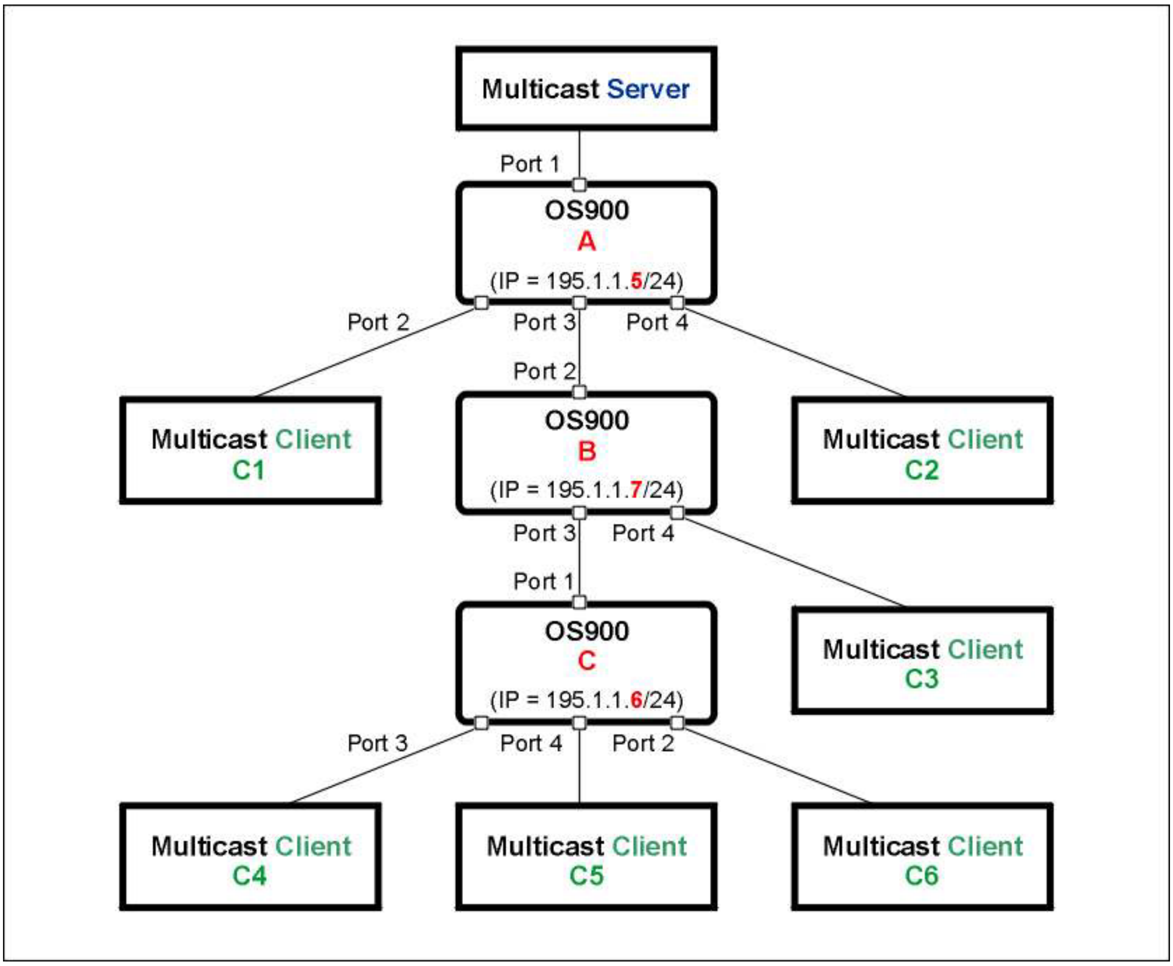



**Figure 48: IGMP IP Multicast Configuration Network Example**

The detailed configuration procedure for each OS900 in *Figure 48*, page *573*, is given below.

OS900 A Configuration

1. Create a VLAN interface (e.g., `vif10`) that includes:
   a. Ports **1**, **2**, **3**, and **4**
      (These ports are to be members of a multicast group. Other ports as well may be included in the VLAN interface.)
   b. A VLAN tag (e.g., **30**)
   c. An IP address (e.g., **195.1.1.5/24**).
2. Enable IGMP on the interface, as described in the section *Enabling IGMP Multicast for a VLAN Interface*, page *562*.
3. Enable IGMP multicast, as described in the section *Enabling IGMP Multicast*, page *560*.
4. Create a multicast group with IP address (e.g., **234.1.8.6**), tag **30**, and ports **2** and **4**, as described in the section *Creating Static Multicast Group(s)*, page *564*.

OS900 B Configuration

1. Create a VLAN interface (e.g., `vif20`) that includes:
   a. Ports **2**, **3**, and **4**
      (These ports are to be members of a multicast group. Other ports as well may be included in the VLAN interface.)
   b. A VLAN tag (e.g., **30**)
   c. An IP address (e.g., **195.3.1.7/24**).

2. Enable IGMP on the interface, as described in the section *Enabling IGMP Multicast for a VLAN Interface*, page *562*.
3. Enable IGMP multicast, as described in the section *Enabling IGMP Multicast*, page *560*.
4. Create a multicast group with IP address (e.g., **`234.1.8.6`**), tag **`30`**, and port **`4`**, as described in the section *Creating Static Multicast Group(s)*, page *564*.
5. Set Port **`3`** to Query Port, as described in the section *Querier Port*, page *566*.
6. Set Port **`3`** to static Non-Server Port, as described in the section *Non-Server Port*, page *567*.

OS900 **C** Configuration

1. Create a VLAN interface (e.g., **`vif30`**) that includes:
   a. Ports **`1`**, **`3`**, **`4`**, and **`2`**
   (These ports are to be members of a multicast group. Other ports as well may be included in the VLAN interface.)
   b. A VLAN tag (e.g., **`30`**)
   c. An IP address (e.g., **`195.2.1.6/24`**).
2. Enable IGMP on the interface, as described in the section *Enabling IGMP Multicast for a VLAN Interface*, page *562*.
3. Enable IGMP multicast as described in the section *Enabling IGMP Multicast*, page *560*.
4. Create a multicast group with IP address (e.g., **`234.1.8.6`**), tag **`30`**, and ports **`3`**, **`4`**, and**`2`**, as described in the section *Creating Static Multicast Group(s)*, page *564*.
5. Set port **`1`** to static Server Port, as described in the section *Server Port*, page *567*.

Execution of the procedure using the OS900 CLI is as follows:

## OS900-A

```
MRV OptiSwitch 910-M version d0733-08-01-06
OS900-A login: admin
Password:

OS900-A> enable
OS900-A# configure terminal

OS900-A(config)# interface vlan vif10
OS900-A(config-vif10)# ports 1-4
OS900-A(config-vif10)# tag 30
Interface is activated.
OS900-A(config-vif10)# ip 195.1.1.5/24
OS900-A(config-vif10)# igmp-enable
OS900-A(config-vif10)# exit

OS900-A(config)# igmp
OS900-A(config-igmp)# enable

OS900-A(config-igmp)# mc-group address 234.1.8.6 tag 30 ports 2,4
Number of multicast groups is 1.
OS900-A(config-igmp)# exit

OS900-A(config-igmp)# show igmp-port 3

Ports  QUERIER         SERVER
-----------------------------------
 3     YES (dynamic)   NO  (dynamic)

OS900-A(config-igmp)# show igmp-port 4

Ports  QUERIER         SERVER
-----------------------------------
 4     YES (dynamic)   NO  (dynamic)

OS900-A(config-igmp)# exit
OS900-A(config)#
```

### OS900-B

```
MRV OptiSwitch 910-M version d0733-08-01-06
OS900-B login: admin
Password:

OS900-B> enable
OS900-B# configure terminal

OS900-B(config)# interface vlan vif20
OS900-B(config-vif20)# ports 2-4
OS900-B(config-vif20)# tag 30
Interface is activated.
OS900-B(config-vif20)# ip 195.1.1.7/24
OS900-B(config-vif20)# igmp-enable
OS900-B (config-vif20)# exit

OS900-B(config)# igmp
OS900-B(config-igmp)# enable

OS900-B(config-igmp)# mc-group address 234.1.8.6 tag 30 ports 4
OS900-B(config-igmp)# port querier static 3
OS900-B(config-igmp)# port not-server static 3

OS900-B(config-igmp)# show igmp-port 3

Ports  QUERIER         SERVER
-----------------------------------
 3     YES (static)    NO  (static)

OS900-B(config-igmp)# exit
OS900-B(config)#
```

## OS900-C

```
MRV OptiSwitch 910-M version d0733-08-01-06
OS900-C login: admin
Password:

OS900-C> enable
OS900-C# configure terminal

OS900-C(config)# interface vlan vif30
OS900-C(config-vif30)# ports 1-4
OS900-C(config-vif30)# tag 30
Interface is activated.
OS900-C(config-vif30)# ip 195.1.1.6/24
OS900-C(config-vif30)# igmp-enable
OS900-C(config-vif30)# exit

OS900-C(config)# igmp
OS900-C(config-igmp)# enable

OS900-C(config-igmp)# mc-group address 234.1.8.6 tag 30 ports 2-4

OS900-C(config-igmp)# port server static 1

OS900-C(config-igmp)# show igmp-port 1

Ports  QUERIER         SERVER
-----------------------------------
 1     YES (dynamic)   YES (static)

OS900-C(config-igmp)# show mc-ip table

Codes of the Flags: I - IGMP registration, S - Static registration.
   Group-IP     num-IFs Flags Tag  Vidx Flags num-Ports PORTs
--------------------------------------------------------------------
 234.1.8.6         1       S
                              30   4097  S    3         2-4
-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
Number of entries: 1
OS900-C(config-igmp)# exit
OS900-C(config)#
```

# Chapter 36: Static and Dynamic Routing

## General

Routing protocols are essentially a set of distributive algorithms used by routers to determine how to forward packets. A routing protocol determines the path and specifies how routers communicate and share information with each other. In addition to or instead of configuring static predetermined routes, any of various on-board routing protocols can be run to enable the network to act dynamically and switch paths as required.

*Figure 49*, below, shows the classification and hierarchy of routing protocols that are supported by the OS900.

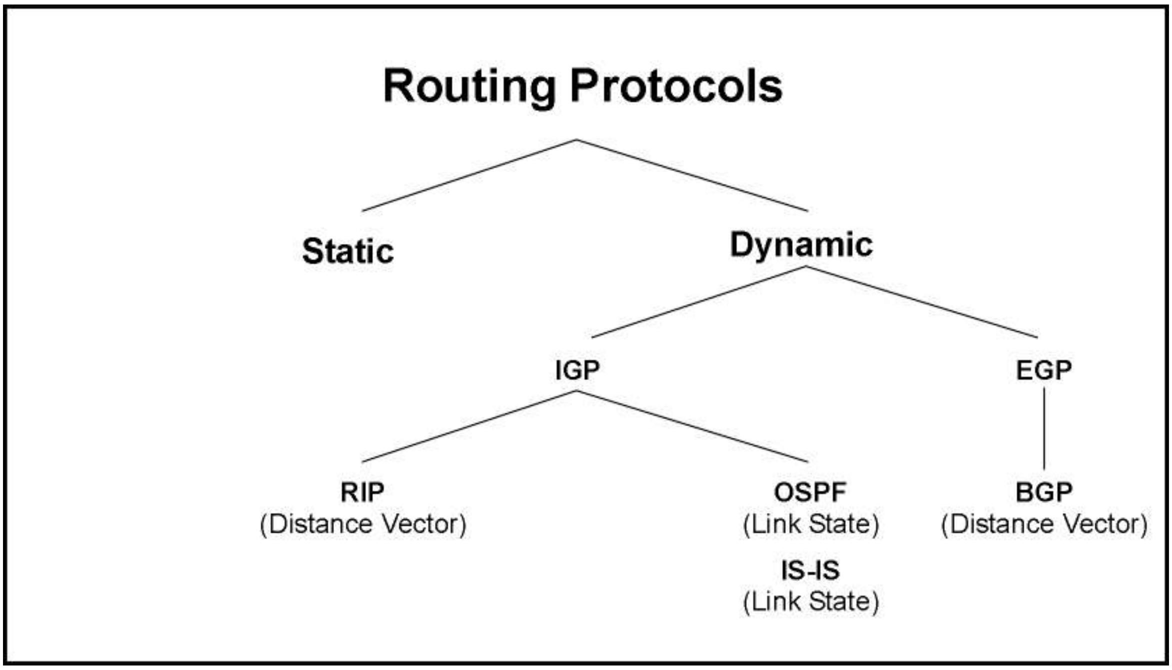



**Figure 49: Routing Protocols – Classification and Hierarchy**

IP routing is the selection of a preferred path for forwarding packets from one IP network to another. IP networks are logical networks, therefore associations of one or more IP networks with an interface is possible. When a host on an IP network needs to send a data packet to a host on another IP network, the source host sends the packet to an IP router or gateway on its local network. The IP router forwards this packet to the destination host's network, or to an intermediary router along the path to the destination. The packet may be handled by several intermediary routers before it reaches the destination network.

MRV's Master-OS™ software suit supports all four IETF-standard-based dynamic routing protocols: RIP, OSPF, IS-IS, and BGP.

The user can configure all or part of this set of protocols concurrently. Following the run of a specific routing protocol, the protocol's local database is filled with entries representing forwarding directions for all learned subnets in the network. Data from these local databases is then propagated to a general routing table called RIB (Routing Information Base) that aggregates information from all protocols as well as from static route entries. The information collected in the RIB contains only L3 data. In order to actually perform forwarding of packets between any two routers, a router needs to synchronize this data with additional L2 data collected in other databases mentioned in this user manual (such as the 'Learning Table'). The synchronized database is called FIB (Forwarding Information Base).

To view statistical information on a protocol's pseudo-threads (average time of run, maximum time of run, number of times the thread was called, etc.), refer to the section *MPLS and Routing Performance*, page *771*.

# Static Routes

A static route is a permanent transmission path for sending data packets to another network. The route remains in IP routing tables until either of the following occurs:

– The administrator deletes it.

– The interface used to reach the next hop in the static route becomes disabled.

To configure a static route for an OS900:

1. Enter **configure terminal** mode.

Example

```
OS900> enable
OS900# configure terminal
```

2. Invoke the command:

**ip route A.B.C.D/M A.B.C.D [1-255]**

where,

**A.B.C.D/M**: IP destination prefix (address/mask) of an ingress packet. Enter 0.0.0.0/0 to enable any packet whose destination address is not present in the IP routing table to be forwarded via the IP gateway. The mask can be up to 31 bits long.

**A.B.C.D**: IP gateway address (next hop IP address)

**[1-255]**: Range of distance values from which one is to be selected for this route

Example

```
OS900(config)# ip route ?
  default-gateway  Default gateway
  A.B.C.D/M        IP destination prefix (e.g. 10.0.0.0/8)
  A.B.C.D          IP destination prefix
OS900(config)# ip route 39.1.2.3/18 ?
  A.B.C.D    IP gateway address
  INTERFACE  IP gateway interface name
  null       Blackhole route
OS900(config)# ip route 39.1.2.3/18 44.44.44.44 ?
  <cr>
  <1-255>  Distance value for this route
  |        Output modifiers
OS900(config)# ip route 39.1.2.3/18 44.44.44.44 7
OS900(config)#OS900(config)#
```

3. Blackhole (Null) Routes

A blackhole (or null) route is a network route (routing table entry) that does not have a real destination. A mechanism in the OS900 can be activated to drop packets on such routes thereby functioning as a kind of firewall. The advantage of this type of firewall over the conventional ones is that it adds virtually no overhead.

To *activate* the blackhole route mechanism for a specific destination prefix:

3.1 Enter **configure terminal** mode.

3.2 Invoke either of the following commands:

**ip route A.B.C.D A.B.C.D null [1-255]**

**ip route A.B.C.D/M null [1-255]**

where,

**A.B.C.D**: (First appearance) *IP destination prefix* (address) of ingress packets to be dropped.

**`A.B.C.D`**: (Second appearance) *IP destination prefix mask* of ingress packets to be dropped.
For example, if the *IP destination prefix* is set as **`3.3.3.3`** and the *IP destination prefix mask* is set as **`255.255.255.0`** then this means all hosts whose IP addresses are in the range **`3.3.3.0`** to **`3.3.3.255`**.

**`A.B.C.D/M`**: IP destination prefix (address/mask) of ingress packets to be dropped.

**`[1-255]`**: Range of distance values from which one is to be selected for this route. Each protocol has a pre-specified distance value. For example, OSPF has the distance value 110, Static routes have the distance value 1. A lower distance value designates a higher priority.

To *deactivate* the blackhole route mechanism for a specific destination prefix:

Enter **`configure terminal`** mode.

Invoke either of the following commands:

```
no ip route A.B.C.D A.B.C.D null [1-255]
no ip route A.B.C.D/M null [1-255]
```

# Dynamic Routes

A dynamic route is a routing entry learned via a routing protocol. Dynamic routing performs the same function as static routing except it is more robust. Static routing allows routing tables in specific routers to be set up manually so network routes for packets are preset. If a router on the route goes down the destination may become unreachable. Dynamic routing allows routing tables in routers to change as the possible routes change.

Routing protocols are usually classified under either one of the following: IGP (Interior Gateway Protocol) and EGP (Exterior Gateway Protocol). IGP are the routing protocols responsible for enabling dynamic routing within the same Autonomous System (AS), i.e. a collection of connected routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet (see RFC 1930, Section 3). EGPs are the set of protocols used between routers of different ASs.

The IETF-standard routing protocols: RIP, OSPF, and IS-IS belong to the IGP group. BGP, on the other hand, belongs to the EGP group – see *Figure 49*, page *579*.

An alternate classification in use for the dynamic routing protocols is Link State or Distance Vector. Distance-vector protocols are those which periodically advertise how far it is (usually in terms of the number of hops) to any known subnet within the network. They do this by advertising a vector of destinations and costs that contains information on all currently known subnets. Any received distance-vector is compared with the local information contained in the protocol's RIB. When a “shorter” distance to a subnet is found this new distance and its compatible next hop are registered directly in the protocol's RIB.

RIP is a good example of a distance-vector routing protocol.

Though BGP is not strictly a distance vector it is usually attributed to be being such a one – see http://en.wikipedia.org/wiki/Routing_Information_Protocol.

A Link-state protocol is one in which a router advertises information about all the links to which it is attached and their compatible state (Up / Down). Using the link-state information a router can build a graph which represents the topology of the overall network. By running a “Shortest Path First” (SPF) Algorithm on the created graph each router can calculate the shortest accumulated distance (path) to any subnet and to install it in its local RIB. Examples of link-state protocols include OSPF and IS-IS.

## Routing Information Protocol (RIP)

### General

RIP is an IGP distance-vector routing protocol. It is using a simple hop count to describe the distance to every sub network it knows within the general network. A hop is a link between two routers on differing networks, i.e., having differing net Ids. The maximum distance to any rip learned subnet cannot exceed 15 hops. The OS900 supports both RIP-I and RIP-II, the latter including subnet masking. Using RIP, the router maintains a routing table and sends it periodically to the closest neighboring routers, so that all the routers running RIP will have the same routing information.

### Configuration

To configure an OS900 to operate with RIP protocol:

1. Enter **configure terminal** mode.

   Example
   ```
   OS900> enable
   OS900# configure terminal
   OS900(config)#
   ```
2. Select RIP as the routing protocol by entering **router rip** mode.

   Example
   ```
   OS900(config)# router rip
   OS900(config-rip-router)#
   ```
3. Enable RIP on the network by invoking the command:

   **network A.B.C.D/M**

   where,

   **A.B.C.D/M**: IP prefix (network/mask), e.g., **35.0.0.0/8**. The mask can be up to 31 bits long.

   Example
   ```
   OS900(config-rip-router)# network 33.3.3.3/16
   OS900(config-rip-router)#
   ```
4. Set the RIP version by invoking the command:

   **version <1-2>**

   where,

   **<1-2>**: RIP versions. (Default is **2**.)

   Example
   ```
   OS900(config-rip-router)# version 1
   OS900(config-rip-router)#
   ```
5. Set a metric for redistributing routes by invoking the command:

   **default-metric <1-16>**

   where,

   **<1-16>** Default metric

   Example
   ```
   OS910(config-router)# default-metric 7
   OS910(config-router)#
   ```
6. Advertise the default gateway route by invoking the command:

   **default-information originate**

   Example
   ```
   OS900(config-router)# default-information originate
   OS900(config-router)#
   ```
7. To set the distance for a specific route, invoke the command:

   **distance <1-255>**

   where,

   **<1-255>**: Distance

   Example
   ```
   OS910(config-router)# distance 5
   OS910(config-router)#
   ```
8. To specify the networks to be excluded from routing updates, invoke the command:

   **distribute-list (prefix WORD|WORD) in|out WORD**

   where,

**prefix WORD**: Name of ACL matching a list of IP prefixes to be excluded from routing updates

**WORD**: (first appearance) Name of an ACL (access list, e.g., **ACL1**) specifying networks to be excluded from routing updates

**in**: Filter (prevent) *incoming* routing updates

**out**: Filter (prevent) *outgoing* routing updates

**WORD**: (second appearance) ID of an existing interface, e.g., **vif5**

Example

```
OS910(config-router)# distribute-list ACL1 out vif5
OS910(config-router)#
```

9. To set the maximum number of RIP routes, invoke the command:

**maximum-prefix <1-65535>**

where,

**<1-65535>**: Maximum number of RIP routes

**<1-100>**: Percentage of maximum routes to generate a warning (default is 75%)

Example

```
OS910(config-router)# maximum-prefix 895 34
OS910(config-router)#
```

10. To specify the router neighbors, invoke the command:

**neighbor A.B.C.D**

where,

**A.B.C.D**: Neighbor IP address

Example

```
OS910(config-router)# neighbor 192.1.23.4
OS910(config-router)# neighbor 192.1.105.8
OS910(config-router)# neighbor 192.1.26.73
OS910(config-router)#
```

11. To suppress routing updates on one or more interface, invoke the command:

**passive-interface IFNAME**

where,

**IFNAME**: ID of an existing interface (e.g., **vif94**)

Example

```
OS910(config-router)# passive-interface vif10
OS910(config-router)#
```

12. To set the size of the buffer that receives RIP UDP packets, invoke the command:

**recv-buffer-size <8192-2147483647>**

where,

**<8192-2147483647>**: Size (in bytes) of buffer that receives RIP UDP packets

Example

```
OS910(config-router)# recv-buffer-size 10000000
OS910(config-router)#
```

13. To enable redistribution of the router's locally connected interface routes, invoke the command:

**redistribute connected**

Example

```
OS900(config-rip-router)# redistribute connected
OS900(config-rip-router)#
```

14. To enable redistribution of the router's local static routes, invoke the command:

**redistribute static**

Example

```
OS900(config-rip-router)# redistribute static
OS900(config-rip-router)#
```

15. To enable redistribution of the router's BGP routes, invoke the command:

    **redistribute bgp [metric <0-16>] [route-map WORD]**

    where,

    **<1-16>** Range of metric values

    **WORD** Name of a route-map

Example

```
OS910(config-router)# redistribute bgp metric 13 route-map Bongo
OS910(config-router)#
```

16. To enable redistribution of the router's kernel routes, invoke the command:

    **redistribute kernel [metric <0-16>] [route-map WORD]**

    where,

    **<1-16>** Range of metric values

    **WORD** Pointer to route-map entries

Example

```
OS910(config-router)# redistribute kernel metric 7 route-map Elephant
OS910(config-router)#
```

17. To enable redistribution of the router's OSPF routes, invoke the command:

    **redistribute ospf [metric <0-16>] [route-map WORD]**

    where,

    **<1-16>** Range of metric values

    **WORD** Pointer to route-map entries

Example

```
OS910(config-router)# redistribute ospf metric 9 route-map Pluto
OS910(config-router)#
```

18. To modify the RIP metric, invoke the command:

    **offset-list WORD in|out <0-16> IFNAME**

    where,

    **WORD** Access-list name, e.g., **ACL2**

    **in**: *Incoming* routing updates

    **out**: *Outgoing* routing updates

    **<0-16>** Range of metric values, e.g., **7**

    **IFNAME**: ID of an existing interface (e.g., **vif6**)

Example

```
OS910(config-router)# offset-list ACL2 out 7 vif6
OS910(config-router)#
```

19. To adjust the routing timers, invoke the command:

    **timers basic <1-2147483647> <1-2147483647> <1-2147483647>**

    where,

    **<1-2147483647>** (first appearance) Routing table update timer value in second. Default: **30**

    **<1-2147483647>** (second appearance) Routing information timeout timer. Default: **180**

    **<1-2147483647>** (third appearance) Garbage collection timer. Default: **120**

Example

```
OS910(config-router)# timers basic 60 300 200
OS910(config-router)#
```

20. To advertise a static route (for debugging purpose), invoke the command:

**route A.B.C.D/M**

where,

**A.B.C.D/M** IP prefix <network>/<length>

Example

```
OS910(config-router)# route 3.3.3.3/22
OS910(config-router)#
```

Below is an example showing how an OS900 can be configured to operate with RIP.

```
OS900# configure terminal
OS900(config)# router ?
  rip  Routing Information Protocol (RIP)
OS900(config)# router rip
OS900(config-router)# network ?
  A.B.C.D/M  IP prefix <network>/<length>,  e.g.,  35.0.0.0/8
  WORD       Interface name
OS900(config-router)# network 25.3.4.7/18
OS900(config-router)# version ?
  <1-2>  version
OS900(config-router)# version 1
OS900(config-router)# redistribute connected
OS900(config-router)# redistribute static
OS900(config-router)#
```

### Authentication Customization

The OS900 provides per interface authentication for RIP messages sent and received by the router. The router reads the RIP message and, if the correct authentication string or password is included, authenticates it. Otherwise, it drops the message. In this way, unauthorized packets are prevented from being processed.

To activate RIP authentication for an OS900:

1. Enter **configure terminal** mode.

Example

```
OS900> enable
OS900# configure terminal
```

2. Enter the mode of a configured VLAN interface by invoking the command:

**interface IFNAME**

where,

**IFNAME**: Interface ID

Example

```
OS900(config)# interface vif3
OS900(config-vif3)#
```

3. Invoke the command:

**ip rip authentication key-chain|mode|string LINE**

where,

**key-chain**: *Key-chain* method for authentication of RIP messages to the router

**mode**: *Mode* method for authentication of RIP messages to the router

**string**: *String* method for authentication of RIP messages to the router

**LINE**: Name of key-chain

Example

```
OS900(config-if)# ip rip authentication key-chain Key_Chain_1
OS900(config-if)#
```

Below is an example showing how RIP authentication can be activated for an OS900.

```
OS900> enable
OS900# configure terminal
```

```
OS900(config)# interface
OS900(config)# interface vif1
OS900(config-if)# ip rip authentication key-chain 22
OS900(config-if)# ip rip authentication mode Main_Floor
OS900(config-if)# ip rip authentication string 12345
OS900(config-if)#
```

## Open Shortest Path First (OSPF)

This section is provided to enable the user to understand the basic OSPF routing principles. OSPF is commonly used in large service provider networks or large financial institutions. The section assumes knowledge of IP routing principles and in particular link-state routing protocols.
The section starts by covering the basic OSPF concepts. It then briefly explains why OSPF is considered an improved routing protocol over Routing Information Protocol (RIP) by indicating how OSPF discovers, chooses, and maintains routing tables.
A few practical scenarios, included in the section, help your complete understanding and ensure you have all the basic OSPF routing skills to complement your understanding of how to configure and maintain OSPF on MRV Master-OS™ in the OS900.

### Basic OSPF

OSPF is a link-state routing protocol. Link-state protocols use the shortest path first (SPF) algorithm to populate the routing table. OSPF shares information with every router in the network. OSPF is considered a difficult protocol to configure and requires a thorough understanding of terms that are commonly used. *Table 22*, below, describes OSPF terminology used in this section.

**Table 22: OSPF Terminology**

| Term | Meaning |
|---|---|
| Link state | Information is shared between directly connected routers. This information propagates throughout the network unchanged and is also used to create a shortest path first (SPF) tree. |
| Area | A group of routers that share the same area ID. All OSPF routers require area assignments. |
| Autonomous system (AS) | A network under a common network administration. |
| Cost | The routing metric used by OSPF. Lower costs are always preferred. You can manually configure the cost with the **ip ospf cost** command. |
| Router ID | Each OSPF router requires a unique router ID. It is recommended to manually assign the router ID. |
| Adjacency | When two OSPF routers have exchanged information between each other and have the same topology table. An adjacency can have the following different states or exchange states:<br>1. **Init state –** When Hello packets have been sent and are awaiting a reply to establish 2-way communication.<br>2. **Establish bi-directional (2-way) communication –** Accomplished by the discovery of the Hello protocol routers and the election of a DR.<br>3. **Exstart –** Two neighbor routers form a master/slave relationship and agree upon a starting sequence to be incremented to ensure LSAs are acknowledged.<br>4. **Exchange state –** Database Description (DD) packets continue to flow as the slave router acknowledges the master's packets. OSPF is operational because the routers can send and receive LSAs between each other. DD packets contain information, such as the router ID, area ID, checksum, if authentication is used, link-state type, and the advertising router. LSA packets contain information, such as router ID also but in addition include MTU sizes, DD sequence numbering, |

| | |
|---|---|
| | and any options.<br>5. **Loading state –** Link-state requests are sent to neighbors asking for recent advertisements that have not yet been discovered.<br>6. **Full state –** Neighbor routers are fully adjacent because their link-state databases are fully synchronized. Routing tables begin to be populated. |

**Table 22: OSPF Terminology** (Cont'd)

| Term | Meaning |
|---|---|
| Topology table | Also called the link-state table. This table contains every link in the whole network. |
| Designated router (DR) | This router is responsible for ensuring adjacencies between all neighbors on a multi-access network (such as Ethernet). This ensures all routers do not need to maintain full adjacencies with each other.<br>The DR is selected based on the router priority. In a tie, the router with the highest router ID is selected. |
| Backup DR | A backup router designed to perform the same functions in case the DR fails. |
| Link-state advertisement (LSA) | A packet that contains all relevant information regarding a router's links and the state of those links. |
| Priority | Sets the router's priority so a DR or BDR can be correctly elected. |
| Router links | Describe the state and cost of the router's interfaces to the area. Router links use LSA type 1. |
| Summary links | Originated by area border routers (ABRs) and describe networks in the AS. Summary links use LSA types 3 and 4. |
| Network links | Originated by DRs. Network links use LSA type 2. |
| External links | Originated by autonomous system boundary routers (ASBRs) and describe external or default routes to the outside (that is, non-OSPF) devices for use with redistribution. External Links use the LSA type 5. |
| Area border router (ABR) | Router located on the border of one or more OSPF areas that connects those areas to the backbone network. |
| Autonomous system boundary router (ASBR) | ABR located between an OSPF autonomous system and a non-OSPF network. |

Before covering various OSPF scenarios, this section covers how OSPF is configured in single and multiple OSPF areas.

### Configuring Basic OSPF Parameters

Enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range.

1. Enter global configuration mode by invoking the command:
   **`configure terminal`**
2. Enable OSPF routing by invoking the command:
   **`router ospf <0-65535>`**
   where,
   `<0-65535>:` OSPF process ID. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value.
3. Set OSPF router ID in IP address format by invoking the command:
   **`router-id A.B.C.D`**

where,

**A.B.C.D:** A.B.C.D OSPF router-ID in IP address format.

4. Define an interface on which OSPF runs and the area ID for that interface by invoking the command:

   **network A.B.C.D/M area <0-4294967295>**

   where,

   **A.B.C.D/M:** A.B.C.D/M OSPF network prefix. (You can use the mask to use a single command to define one or more multiple interfaces to be associated with a specific OSPF area. The area ID can be a decimal value or an IP address.) The mask can be up to 31 bits long.

The example below shows how to configure an OSPF routing process and assign it a process number.

Example

```
router ospf 1
ospf router-id 0.0.0.1
network 192.168.1.0/30 area 1
```

**Configuring Interface-specific OSPF Parameters**

You can use the IP OSPF configuration commands to modify interface-specific OSPF parameters. You are not required to modify any of these parameters, but some interface parameters (hello, interval, dead interval, and authentication key) must be consistent across all routers in an attached network. If you modify these parameters, **make sure all routers in the network have compatible values.**

1. Enter global configuration mode by invoking the command:

   **configure terminal**

2. Enter VLAN interface configuration mode by invoking the command:

   **interface vlan IFNAME**

   where,

   **IFNAME:** Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095.

3. (Optional) Explicitly specify the cost of the interface by invoking the command:

   **ip ospf cost <1-65535>**

   where,

   **<1-65535>:** Cost

4. (Optional) Specify the number of seconds between link state advertisement transmissions by invoking the command:

   **ip ospf retransmit-interval <3-65535>**

   where,

   **<3-65535>:** IP OSPF retransmit-interval in seconds. Default: 5 seconds.

5. (Optional) Set priority to help find the OSPF designated router for a network by invoking the command:

   **ip ospf priority <0-255>**

   where,

   **<0-255>:** IP OSPF priority. Default: 1.

6. (Optional) Set the number of seconds between hello packets sent on an OSPF interface by invoking the command:

   **ip ospf hello-interval <1-65535>**

   where,

   **<1-65535>:** IP OSPF hello-interval <1-65535>. The value must be the same for all nodes on a network. Default: 10 seconds.

7. (Optional) Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down by invoking the command:

   **`ip ospf dead-interval <1-65535>`**

   where,

   **`<1-65535>:`** The range of values (in seconds). The value must be the same for all nodes on a network. Default: 4 times the hello interval.

8. (Optional) Enable MD5 authentication by invoking the command:

   **`ip ospf message-digest-key <1-255> md5 KEY`**

   where,

   **`<1-255>:`** Key ID.

   **`KEY:`** The OSPF password (key). (An alphanumeric password of up to 16 bytes.)

The example below shows how to configure OSPF hello interval, dead-interval, and cost.

Example

```
R1# configure  terminal
R1(config)#
R1(config)# interface  vif2
R1(config-vif2)#
R1(config-vif2)# ip ospf  hello-interval  1
R1(config-vif2)#
R1(config-vif2)# ip ospf  dead-interval 4
R1(config-vif2)#
R1(config-vif2)# ip ospf  cost  1000
```

**Configuring OSPF Area Parameters**

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution. Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the area range router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

1. Enable OSPF routing, and enter router configuration mode by invoking the command:

   **`router ospf <0-65535>`**

   where,

   **`<0-65535>:`** OSPF process ID. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value.

2. (Optional) Allow password-based protection against unauthorized access to the identified area by invoking the command:

   **`area <0-4294967295> authentication`**

   where,

   **`<0-4294967295>:`** OSPF area ID as a decimal value.

3. (Optional) Define an area as a stub area by invoking the command:

   **`area <0-4294967295> authentication message-digest`**

   where,

   **`<0-4294967295>:`** OSPF area ID as a decimal value.

   **`message-digest:`** Enables message digest 5 (MD5) authentication on the area specified by the OSPF area ID.

4. (Optional) Define an area as a not-so-stubby-area by invoking the command:

   **`area <0-4294967295> nssa [no-redistribution]|[default-information-originate]|[no-summary]`**

   where,

   **`nssa:`** Configure OSPF area as NSSA. Every router within the same area must agree that the area is NSSA.

   **`<0-4294967295>:`** OSPF area ID as a decimal value.

   **`no-redistribution:`** Do not redistribute ext. routes to the NSSA area. Select when the router is an NSSA ABR and you want the redistribute command to import routes into normal areas, but not into the NSSA.

   **`default-information-originate:`** Originate default information to the NSSA area. Select on an ABR to allow importing type 7 LSAs into the NSSA.

   **`no-summary:`** Do not inject inter-area routes into NSSA. Select to not send summary LSAs into the NSSA..

5. (Optional) Specify an address range for which a single route is advertised. by invoking the command:

   **`area <0-4294967295> range A.B.C.D/M`**

   where,

   **`<0-4294967295>:`** OSPF area ID as a decimal value.

   **`A.B.C.D/M:`** area range prefix.

   Use this command only with area border routers.

### Configuring Other OSPF Parameters

You can optionally configure other OSPF parameters in router configuration mode

1. Using Route Maps to Redistribute Routing Information

   The OS900 can run multiple routing protocols concurrently, and it can redistribute information from one routing protocol to another. Redistributing information from one routing protocol to another applies to all supported IP-based routing protocols.

   You can also conditionally control the redistribution of routes between routing domains by defining enhanced packet filters or route maps between the two domains. The match and set route-map configuration commands define the condition portion of a route map. The match command specifies that a criterion must be matched. The set command specifies an action to be taken if the routing update meets the conditions defined by the match command. Although redistribution is a protocol-independent feature, some of the match and set route-map configuration commands are specific to a particular protocol.

   a. Enter global configuration mode by invoking the command:

      **`configure terminal`**

   b. Define any route maps used to control redistribution and enter route-map configuration mode by invoking the command:

      **`route-map WORD (deny|permit) <1-65535>`**

      where,

      **`WORD:`** Route map tag.

      **`deny:`** Route map denies set operations. If deny is specified, the route is not redistributed.

      **`permit:`** Route map permits set operations. If permit is specified and the match criteria are met for this route map, the route is redistributed as controlled by the set actions.

      **`[<1-65535>]:`** Sequence to insert to/delete from existing route-map entry. It indicates the position a new route map is to have in the list of route maps already configured with the same name.

   c. Match a standard access list by specifying the name or number by invoking one of the commands:

      **`match ip address WORD`**

      where,

**WORD:** IP access-list name.

**match ip address prefix-list WORD**

where,

**WORD:** IP prefix-list name.

d. Match a next-hop router address passed by one of the access lists specified by invoking one of the commands:

**match ip next-hop WORD**

where,

**WORD:** IP access-list name.

**match ip next-hop prefix-list WORD**

where,

**WORD:** IP prefix-list name.

e. Match the specified interface by invoking the command:

**match interface IFNAME**

where,

**IFNAME:** Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095.

f. Match the specified route-type by invoking the command:

**match route-type external (type-1| type-2)**

where,

**external:** OSPF External route type. (Type 1 or Type 2) external routes.

**type-1:** Match OSPF External Type 1 metrics.

**type-2:** Match OSPF External Type 2 metrics.

The following example shows setting of static routes with Router-map.

Create access-list ZebOS

Example

```
R1(config)# access-list zebos Static permit 172.29.4.10/32
R1(config)# access-list zebos Static permit 172.29.4.11/32
create route-map and match the access-list
R1(config)# route-map static permit 1
R1(config)#match ip address Static
```

Redistribute this route-map in the router ospf as follows:

```
R1(config-router)# redistribute static route-map static
```

2. Virtual links: In OSPF, all areas must be connected to a backbone area. You can establish a virtual link in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the non-backbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.
3. Default route: When you specifically configure redistribution of routes into an OSPF routing domain, the route automatically becomes an autonomous system boundary router (ASBR). You can force the ASBR to generate a default route into the OSPF routing domain.
4. Administrative distance is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. OSPF uses three different administrative distances: routes within an area (inter-area), routes to another area (inter-area), and routes from another routing domain learned through redistribution (external). You can change any of the distance values.
5. Passive interfaces: If a specific network should be taken for OSPF calculations, however the router shouldn't send hello packets on this network interface, this interface should be configured as passive.
6. Route calculation timers: You can configure the delay time between when OSPF

receives a topology change and when it starts the shortest path first (SPF) calculation and the hold time between two SPF calculations.

a. Enter global configuration mode by invoking the command:

   **`configure terminal`**

b. Enable OSPF routing, and enter router configuration mode by invoking the command:

   **`router ospf <0-65535>`**

   where,

   **`<0-65535>:`** OSPF process ID. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value.

c. (Optional) Specify an address and IP subnet mask for redistributed routes so that only one summary route is advertised by invoking the command:

   **`summary-address A.B.C.D/M`**

   where,

   **`A.B.C.D/M:`** Summary prefix designated for a range of addresses. The mask can be up to 31 bits long.

d. (Optional) Establish a virtual link and set its parameters by invoking the command:

   **`area <0-4294967295> virtual-link A.B.C.D [dead-interval <1-65535>] [hello-interval <1-65535>] [retransmit-interval <1-65535>] [transmit-delay <1-65535>] [authentication-key AUTH_KEY] [authentication AUTH_KEY] [message-digest-key authentication-key AUTH_KEY]`**

   where,

   **`<1-65535>:`** (First appearance) Dead router detection time in seconds.

   **`<1-65535>:`** (Second appearance) Hello packet interval in seconds.

   **`<1-65535>:`** (Third appearance) LSA retransmit interval in seconds.

   **`<1-65535>:`** (Fourth appearance) LSA transmission delay in seconds.

   **`AUTH_KEY:`** Authentication key (up to 8 characters).

e. (Optional) Force the ASBR to generate a default route into the OSPF routing domain by invoking the command:

   **`default-information originate [always] [metric <0-16777214>] [metric-type 1|2] [route-map WORD]`**

   where,

   **`always:`** Always advertise default route.

   **`<0-16777214>:`** OSPF metric.

   **`1:`** Set OSPF External Type 1 metrics.

   **`2:`** Set OSPF External Type 2 metrics.

   **`WORD:`** Pointer to route-map entries.

f. (Optional) Change the OSPF distance values by invoking the command:

   **`distance ospf (external <1-255>)|(inter-area <1-255>)|(intra-area <1-255>)`**

   where,

   **`<1-255>:`** (First appearance) Distance for external routes. Default: 110.

   **`<1-255>:`** (Second appearance) Distance for inter-area routes. Default: 110.

   **`<1-255>:`** (Third appearance) Distance for intra-area routes. Default: 110.

g. (Optional) Suppress the sending of hello packets through the specified interface by invoking the command:

   **`passive-interface IFNAME`**

   where,

   **`IFNAME:`** Interface ID having the format **`vifX`**, where **`X`** is a decimal number in the range 1-4095.

h. Delay receiving a change to SPF calculation by invoking the command:

**`timers spf <0-4294967295> <0-4294967295>`**

where,

`<0-4294967295>`: (First appearance) Delay between receiving a change to SPF calculation.

`<0-4294967295>`: (Second appearance) Hold time between consecutive SPF calculations.

7. To fix the transmission pace of LSAs (unicast and broadcast), invoke the command:

   Enter **`router ospf`** mode.

   Invoke the command:

   **`timers pacing flood <5-300>`**

   where,

   `<5-300>`: Range of time intervals (in milliseconds) between transmissions of two consecutive LSAs.

   To free the transmission pace of LSAs, invoke the command **`no timers pacing flood`**.

8. To cause the hold-time to be reset for every incoming unicast packet:

   Enter **`router ospf`** mode.

   Invoke the command:

   **`[ospf] prioritized-treatment inactivity-timer`**

   To cancel resetting of hold-time for every incoming unicast packet, invoke the command **`no [ospf] prioritized-treatment inactivity-timer`**.

9. To cause hold-time-related debug information to be printed to the syslog, invoke the command:

   Enter **`configure terminal`** mode.

   Invoke the command:

   **`debug ospf prioritized-treatment inactivity-timer`**

   To prevent printing of hold-time-related debug information to the syslog, invoke the command **`no debug ospf prioritized-treatment inactivity-timer`**.

10. To activate an exponential back-off algorithm for determining the value of the retransmission interval for LSAs.

    Enter **`router ospf`** mode.

    Invoke the command:

    **`prioritized-treatment retransmit-interval <1-7> <3-65535>`**

    where,

    `<1-7>`: **K** parameter of the algorithm for the function R(LSA) = Min(K * R(LSA), Rmax) sec

    `<3-65535>`: Maximum interval Rmax (in seconds) for the function R(LSA) = Min(K * R(LSA), Rmax)

    To deactivate the exponential back-off algorithm, invoke the command **`no prioritized-treatment retransmit-interval`**.

11. To cause retransmission-interval-related debug information to be printed to the syslog, invoke the command:

    Enter **`configure terminal`** mode.

    Invoke the command:

    **`debug ospf prioritized-treatment retransmit-interval`**

    To prevent printing of retransmission-interval-related debug information to the syslog, invoke the command **`no debug ospf prioritized-treatment retransmit-interval`**.

12. To set the rate[74] at which LSAs are sent to a neighbor that is suspected of being congested.

    Enter **`router ospf`** mode.

    Invoke the command:

    **`[ospf] prioritized-treatment lsa-pacing boundaries HIGH LOW gap-factor <1-5> consistency <1-5>`**

    where,

    **`HIGH`**: High Water Mark

    **`LOW`**: Low Water Mark

    **`<1-5>`**: (first appearance) Factor by which gap between successive LSAs is to be increased during congestion Gap-pacing-factor

    **`<1-5>`**: (second appearance) Minimum time that has to elapse before the existing gap is considered for change

    To cancel sending of LSAs to a neighbor that was suspected of being congested, invoke the command **`no prioritized-treatment lsa-pacing`**.

13. To cause LSA-rate-related debug information to be printed to the syslog, invoke the command:

    Enter **`configure terminal`** mode.

    Invoke the command:

    **`debug ospf prioritized-treatment lsa-pacing`**

    To prevent printing of LSA-rate-related debug information to the syslog, invoke the command **`no debug ospf prioritized-treatment lsa-pacing`**.

14. OSPF adjacencies are formed gradually, i.e., no more than the configured maximum amount of adjacencies are formed simultaneously. The user can set the interval during which the OS900 is to retry to establish new adjacencies.
    To set the retry interval:

    Enter **`router ospf`** mode.

    Invoke the command:

    **`[ospf] prioritized-treatment throttling-adjacencies max-num <1-5> [retry-interval <1-20>]`**

    where,

    **`<1-5>`**: Simultaneous adjacencies

    **`<1-20>`**: Number of seconds to wait between consecutive adjacency formation. (Default: 10 seconds)

    To deactivate retry, invoke the command **`no prioritized-treatment throttling-adjacencies`**.

15. To cause retry-interval-related debug information to be printed to the syslog, invoke the command:

    Enter **`configure terminal`** mode.

    Invoke the command:

    **`debug ospf prioritized-treatment throttling-adjacencies`**

    To prevent printing of retry-interval-related debug information to the syslog, invoke the command **`no debug ospf prioritized-treatment throttling-adjacencies`**.

### Monitoring OSPF

You can display specific statistics such as the contents of IP routing tables, caches, and databases.

| Command | Purpose |
|---|---|
| **`show ip ospf <0-65535>`** | Display general information about OSPF |

[74] This rate follows an exponential back-off algorithm described in detail in the application note.

| | |
|---|---|
| where,<br>`<0-65535>`: OSPF process ID | routing processes. |
| **show ip ospf [<0-65535>] database [router] [A.B.C.D]**<br>where,<br>`<0-65535>`: OSPF process ID<br>`A.B.C.D`: Link State ID (as an IP address)<br>**show ip ospf [<0-65535>] database [router] [self-originate]**<br>where,<br>`<0-65535>`: OSPF process ID<br>**show ip ospf [<0-65535>] database [router] [adv-router [A.B.C.D]]**<br>where,<br>`<0-65535>`: OSPF process ID<br>`A.B.C.D`: Advertising router IP address<br>**show ip ospf [<0-65535>] database [network] [A.B.C.D]**<br>where,<br>`<0-65535>`: OSPF process ID<br>`A.B.C.D`: Link State ID (as an IP address)<br>**show ip ospf [<0-65535>] database [summary] [A.B.C.D]**<br>where,<br>`<0-65535>`: OSPF process ID<br>`A.B.C.D`: Link State ID (as an IP address)<br>**show ip ospf [<0-65535>] database [asbr-summary] [A.B.C.D]**<br>where,<br>`<0-65535>`: OSPF process ID<br>`A.B.C.D`: Link State ID (as an IP address)<br>**show ip ospf [<0-65535>] database [external] [A.B.C.D]**<br>where,<br>`<0-65535>`: OSPF process ID<br>`A.B.C.D`: Link State ID (as an IP address)<br>**show ip ospf [process-id area-id] database [database-summary** | Display lists of information related to the OSPF database. |
| **show ip ospf border-routes** | Display the internal OSPF routing ABR and ASBR table entries. |
| **show ip ospf interface [INTERFACE]**<br>where,<br>`INTERFACE`: Interface ID having the | Display OSPF-related interface information |

| | |
|---|---|
| format **vifX**, where **X** is a decimal number in the range 1-4095. | |
| **show ip ospf neighbor [interface A.B.C.D]**<br>where,<br>**A.B.C.D:** Interface IP address. | Display OSPF interface neighbor information |
| **show ip ospf virtual-links** | Display OSPF-related virtual links information. |
| **show ip ospf refresh-list** | Display the different LSA groups created in the refresh-list database. The information can be used for changing the settings of the “refresh-list timers” and for pace the LSAs accordingly during the refresh time period. |

### Configuring OSPF in a Single Area

When configuring any OSPF router, you must establish which area assignment to enable the interface for. OSPF has some basic rules when it comes to area assignment. OSPF must be configured with areas. The backbone area 0, or 0.0.0.0, must be configured if you use more than one area assignment. You can configure OSPF in one area; you can choose any area, although good OSPF design dictates that you configure area 0.

To enable OSPF on a OS900 and advertise interfaces, do the following:

1. Use the command **router ospf** *with a process ID* to start OSPF.
2. Assign the router ID.
3. Use the **network** command to enable the interfaces.
4. Identify area assignments.

Example 1 displays OSPF with a process ID of 1 and places all interfaces configured with an IP address in area 0. The network command **network 192.168.1.0/30 (255.255.255.252) area 0** .

***Example 1: Configuring OSPF in a Single Area***

```
router ospf 1
ospf router-id 0.0.0.1
network 192.168.1.0/30 area 0
```

The following is a list of reasons OSPF is considered a better routing protocol than RIP:

- OSPF has no hop count limitations. (RIP has 15 hops only.)
- OSPF understands variable-length subnet masks (VLSMs) and allows for summarization.
- OSPF uses multicasts (not broadcasts) to send updates.
- OSPF converges much faster than RIP, because OSPF propagates changes immediately.
- OSPF has authentication available. (RIPv2 does also, but RIPv1 does not.)
- OSPF allows for tagging of external routes injected by other autonomous systems.
- OSPF configuration, monitoring, and troubleshooting have a far greater Master-OS™ tool base than RIP.

**Note**

OSPF does have some disadvantages, including the level of difficulty and understanding required to configure, monitor, and troubleshoot it. You can configure more than one OSPF process, but you must be mindful that the SPF calculations associated with multiple OSPF processes can consume a considerable amount of CPU and memory.

### Scenarios

The following scenarios are designed to draw together and further explore the content described earlier in this section and some of the content you have seen in your own networks or practice labs. There is not always one right way to accomplish the tasks presented, and using good practice and defining your end goal are important in any real-life design or solution.

#### *Scenario 1: Configuring OSPF in a Single Area*

In this scenario, you configure two OS900s for OSPF routing using a variable Class network. *Figure 50*, below, shows the IP addressing and area assignments for Routers R1 and R2.

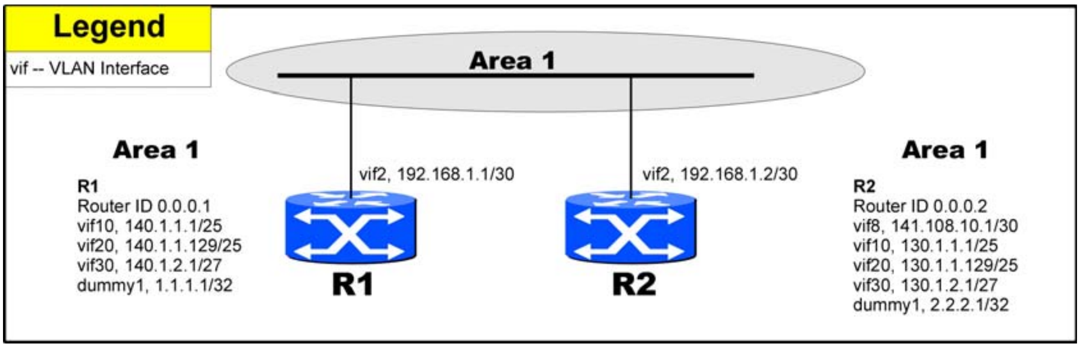



**Figure 50: Basic OSPF**

Configure R1 for OSPF first. Assign all interfaces with the area assignment 1. Note that this scenario uses VLSM. Use the **network** command and match the IP subnet exactly. Example 2 displays the OSPF configuration performed on R1.

> **Note**
> Routers R1 and R2 reside in one area; so, in fact, you could apply the one Master-OS™ command to enable all interfaces configured with an IP address in the range 131.108.0.0 through 131.108.255.255 with the command **network 131.108.0.0 0.0.255.255 area 1.**

**_Example 2: R1 OSPF Configuration_**

```
router ospf 1
 ospf router-id 0.0.0.1
 network 1.1.1.1/32 area 1
 network 140.1.1.0/25 area 1
 network 140.1.1.128/25 area 1
 network 140.1.2.0/27 area 1
 network 192.168.1.0/30 area 1
!
```

Example 3 displays the OSPF configuration performed on R2.

**_Example 3: R2 OSPF Configuration_**

```
router ospf 2
 ospf router-id 0.0.0.2
 network 2.2.2.1/32 area 1
 network 130.1.1.0/25 area 1
 network 130.1.1.128/25 area 1
 network 130.1.2.0/27 area 1
 network 192.168.1.0/30 area 1
!
```

> **Note**
> R1 has a process ID of 1 and R2 has a process ID of 2. The process ID is locally significant only and doesn't need to match between routers. The process ID can be any number between 1–65535.

Example 4 displays the remote networks reachable through OSPF with a cost metric of  for all. The next hop address is 192.168.1.x through Interface vif2

Example 4, which displays the IP routing table on R1.

***Example: 4 R1's IP Routing Table***

```
R1# show ip route  ospf
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info

O    1.1.1.1/32 [110/10] is directly connected, dummy1, 00:04:46
O> * 2.2.2.1/32 [110/11] via 192.168.1.2, vif2, 00:02:25
O> * 130.1.1.0/25 [110/2] via 192.168.1.2, vif2, 00:02:25
O> * 130.1.1.128/25 [110/2] via 192.168.1.2, vif2, 00:02:25
O    140.1.1.0/25 [110/1] is directly connected, vif10, 00:04:36
O    140.1.1.128/25 [110/1] is directly connected, vif20, 00:04:36
O    192.168.1.0/30 [110/1] is directly connected, vif2, 00:04:16
```

***Example 5: Show the IP routing table on R2***

```
R2# show ip route  ospf
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info

O> * 1.1.1.1/32 [110/11] via 192.168.1.1, vif2, 00:10:25
O    2.2.2.1/32 [110/10] is directly connected, dummy1, 00:11:21
O    130.1.1.0/25 [110/1] is directly connected, vif10, 00:11:11
O    130.1.1.128/25 [110/1] is directly connected, vif20, 00:11:11
O> * 140.1.1.0/25 [110/2] via 192.168.1.1, vif2, 00:10:25
O> * 140.1.1.128/25 [110/2] via 192.168.1.1, vif2, 00:10:25
O    192.168.1.0/30 [110/1] is directly connected, vif2, 00:10:
```

***Example 6: Show ip ospf interface vif2 on R1***

```
R1# show ip ospf interface vif2
vif2 (ifindex = 5) is up, line protocol is up
  Internet Address 192.168.1.1/30, Area 0.0.0.1
    Router ID 0.0.0.1, Network Type BROADCAST, Cost: 1, TE Metric 0
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 0.0.0.1, Interface Address 192.168.1.1
    Backup Designated Router (ID) 0.0.0.2, Interface Address 192.168.1.2
    OSPF Interface MTU 1500
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:02
    Neighbor Count is 1, Adjacent neighbor count is 1
    Crypt Sequence Number is 0
```

The cost associated with the path on the Ethernet segment is 10. Therefore, the total cost is 1000 (as advertised by R2) plus 10, which equals 1010. Another method you can use to determine the cost with an Ethernet segment is to use the cost calculation, cost = $10^8$ / Bandwidth = $10^8$ / $10^7$ = 10. Example 7 displays the full routing configuration on R1.

***Example 7: R1 Full Configuration***

```
!
Current configuration:
! version 2_1_1
!
hostname R1
!
interface vlan vif2
 description ** Connection To R2 ***
 tag 2
 ip 192.168.1.1/30
 ports 24
!
interface vlan vif10
 description *** Client Lan Connection **
 tag 10
```

```
 ip 140.1.1.1/25
 ports 1
!
interface vlan vif20
 description *** Client Lan Connection **
 tag 20
 ip 140.1.1.129/25
 ports 3
!
interface vlan vif30
 tag 30
 ip 140.1.2.1/27
 ports 5
!
interface dummy dummy1
 description *** LoopBack Interface ***
 ip 1.1.1.1/32
!
router ospf 1
 ospf router-id 0.0.0.1
 network 1.1.1.1/32 area 1
 network 140.1.1.0/25 area 1
 network 140.1.1.128/25 area 1
 network 140.1.2.0/27 area 1
 network 192.168.1.0/30 area 1
!
```

Example 8 displays the full routing configuration on R2.

***Example 8: R2 Full Configuration***

```
hostname R2
!
interface vlan vif2
 description *** Connection to R1 **
 tag 2
 ip 192.168.1.2/30
 ports 7
!
interface vlan vif10
 description *** Client Lan Connection **
 tag 10
 ip 130.1.1.1/25
 ports 1
!
interface vlan vif20
 description *** Client Lan Connection **
 tag 20
 ip 130.1.1.129/25
 ports 3
!
interface vlan vif30
 description *** Client Lan Connection **
 tag 30
 ip 130.1.2.1/27
 ports 5
 ip ospf network point-to-point
 ip ospf cost 1000
!
interface dummy dummy1
 ip 2.2.2.1/32
!
router ospf 2
 ospf router-id 0.0.0.2
```

```
 network 2.2.2.1/32 area 1
 network 130.1.1.0/25 area 1
 network 130.1.1.128/25 area 1
 network 130.1.2.0/27 area 1
 network 192.168.1.0/30 area 1
!
R2#
```

Now, apply the OSPF principles to a larger, more complex network in Scenario 2.

### *Scenario 2: Configuring OSPF in Multiple Areas*

Turn your attention to a far more complex OSPF scenario and apply some of the advanced features in OSPF.

This scenario uses four routers: R1 and R2 from scenario 1 and two new routers named R4 and R3. *Figure 51*, below, displays the routers in this scenario.

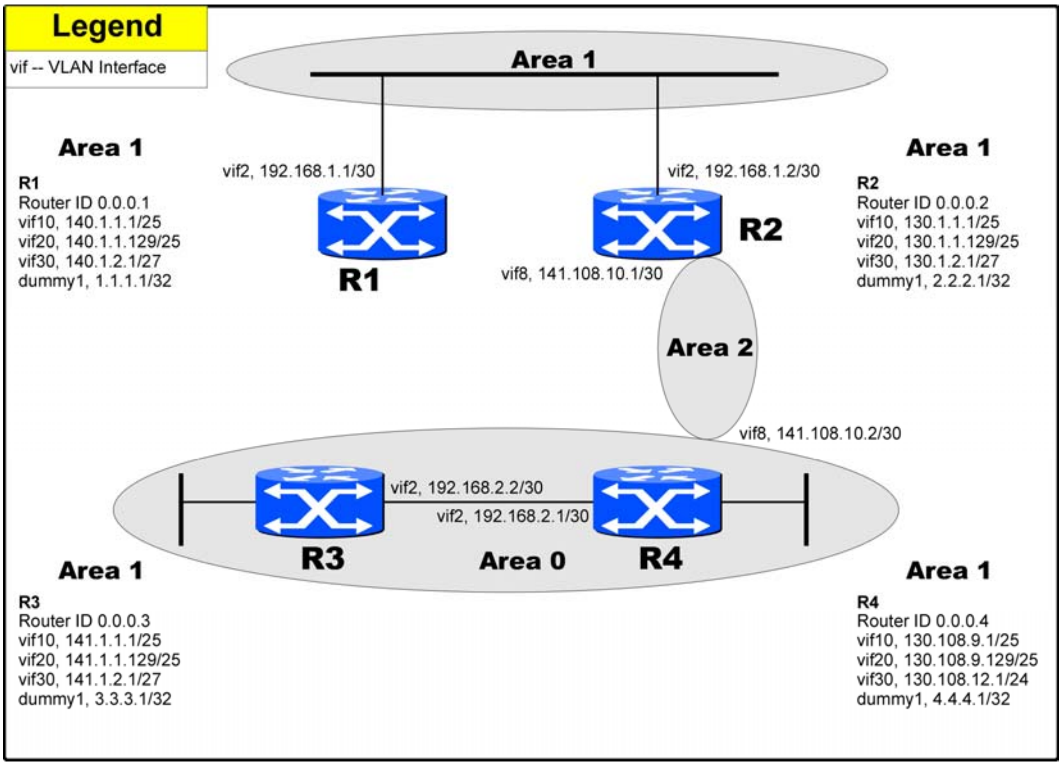



**Figure 51: OSPF Topology and IP Addressing**

In this scenario, you add two new routers, R3 and R4, and create an additional two new areas: Area 0 and Area 2. That makes a total of three areas: the backbone Area 0 between R3 and R4, Area 2 covering the link between R4and R2, and Area 1 covering the Ethernets between R1 and R2.

Routers R2 and R4 in this case are referred to area border routers (ABRs) because more than one area is configured on each router. OSPF includes a number of different router types. *Table 23*, below, displays all the possible routers types.

**Table 23: OSPF Router Types**

| Router type | Description |
|---|---|
| Internal router | This router is within a specific area only. Internal router functions include maintaining the OSPF database and forwarding data to other networks. All interfaces on internal routers are in the same area. |
| Area border router (ABR) | ABRs are responsible for connecting two or more areas. ABRs contain the full topological database of each area they are connected to and send this information to other areas. |
| Autonomous system border router (ASBR) | ASBRs connect to the outside world or perform some form of redistribution into OSPF. |
| Backbone router | Backbone routers are connected to area 0, also know as area 0.0.0.0. Backbone routers can be internal routers and ASBRs. |

In *Figure 51*, above, R1 is an internal router; R2 is an ABR; R4 is a backbone router and ABR, and R3 is a backbone router.

Router R1 requires no configuration change, but you need to modify R2 and enable OSPF on R3 and R4. Example 9 displays the modifications required on R2.

Remember that you have a link to R4, so you need to set IP addressing.

The following example shows configuration of R2 as ABR.

***Example 9: Enable OSPF on R4 with Process ID 6***

```
R2(config)# router ospf  2
R2(config-router)# network  141.108.10.0/30 area 2
```

Now, enable OSPF on R3 and R4. Notice the IP addressing in *Figure 51*, above, has a mixture of the Class B networks 131.108.0.0 and 141.108.0.0 with different subnets.

Hence, this scenario uses VLSM extensively to illustrate the capability of OSPF to handle VLSM.

To enable OSPF on R4, start the OSPF process with the process ID 4 and enable the interfaces to advertise the networks as displayed by Example 10.

***Example 10: Enable OSPF on R4 with Process ID 4***

```
router ospf 4
 ospf router-id 0.0.0.4
 network 4.4.4.1/32 area 0
 network 130.108.9.0/25 area 0
 network 130.108.9.128/25 area 0
 network 130.108.12.0/24 area 0
 network 141.108.10.0/30 area 2
 network 192.168.2.0/30 area 0
```

Similarly, Example 11 displays the OSPF configuration required on R3.

***Example 11: Enable OSPF on R3***

```
router ospf 3
 ospf router-id 0.0.0.3
 network 3.3.3.1/32 area 0
 network 141.1.1.0/25 area 0
 network 141.1.1.128/25 area 0
 network 141.1.2.0/27 area 0
 network 192.168.2.0/30 area 0
```

Now that OSPF is configured on all four routers, examine the routing table on the backbone network to ensure that all networks are routable. Example 12 displays the IP routing table on R4.

***Example 12: IP Routing Table on R4***

```
R4# show ip  route
multipath equal cost limit: 1
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info
```

```
O> * 3.3.3.1/32 [110/11] via 192.168.2.2, vif2, 00:09:15
O    4.4.4.1/32 [110/10] is directly connected, dummy1, 00:09:25
C> * 4.4.4.1/32 is directly connected, dummy1
O    130.108.9.0/25 [110/1] is directly connected, vif10, 00:09:25
C> * 130.108.9.0/25 is directly connected, vif10
O    130.108.9.128/25 [110/1] is directly connected, vif20, 00:08:09
C> * 130.108.9.128/25 is directly connected, vif20
O    130.108.12.0/24 [110/1] is directly connected, vif30, 00:07:54
C> * 130.108.12.0/24 is directly connected, vif30
O> * 141.1.1.0/25 [110/2] via 192.168.2.2, vif2, 00:09:15
O> * 141.1.1.128/25 [110/2] via 192.168.2.2, vif2, 00:07:54
O> * 141.1.2.0/27 [110/2] via 192.168.2.2, vif2, 00:07:43
O    141.108.10.0/30 [110/1] is directly connected, vif8, 00:09:25
C> * 141.108.10.0/30 is directly connected, vif8
O    192.168.2.0/30 [110/1] is directly connected, vif2, 00:09:25
C> * 192.168.2.0/30 is directly connected, vif2
```

Example 12 displays the remote networks on Router R3, but not the networks from R1 or R2. For example, the Ethernet network 140.1.1.1/24 in area 1 is not routable from R4.

Examine R3's routing table. Example 13 displays R3's IP routing table.

***Example 13: R3's IP Routing Table***

```
R3# show ip route
multipath equal cost limit: 1
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info

O    3.3.3.1/32 [110/10] is directly connected, dummy1, 00:25:06
C> * 3.3.3.1/32 is directly connected, dummy1
O> * 4.4.4.1/32 [110/11] via 192.168.2.1, vif2, 00:08:04
O> * 130.108.9.0/25 [110/2] via 192.168.2.1, vif2, 00:08:04
O> * 130.108.9.128/25 [110/2] via 192.168.2.1, vif2, 00:06:57
O> * 130.108.12.0/24 [110/2] via 192.168.2.1, vif2, 00:06:42
O    141.1.1.0/25 [110/1] is directly connected, vif10, 00:24:56
C> * 141.1.1.0/25 is directly connected, vif10
O    141.1.1.128/25 [110/1] is directly connected, vif20, 00:06:42
C> * 141.1.1.128/25 is directly connected, vif20
O    141.1.2.0/27 [110/1] is directly connected, vif30, 00:06:31
C> * 141.1.2.0/27 is directly connected, vif30
O> * 141.108.10.0/30 [110/2] via 192.168.2.1, vif2, 00:08:04
O    192.168.2.0/30 [110/1] is directly connected, vif2, 00:13:40
C> * 192.168.2.0/30 is directly connected, vif2
```

Once more, Example 13 doesn't display the networks in area 1 on Routers R1 and R2. Example 14 displays R2's IP routing table.

***Example 14: R2's IP Routing Table***

```
R2#show ip  route
multipath equal cost limit: 1
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info

O> * 1.1.1.1/32 [110/11] via 192.168.1.1, vif2, 00:13:44
C> * 2.2.2.1/32 is directly connected, dummy1
O    130.1.1.128/25 [110/1] is directly connected, vif20, 00:15:09
C> * 130.1.1.128/25 is directly connected, vif20
O    130.1.2.0/27 [110/1] is directly connected, vif30, 00:04:53
C> * 130.1.2.0/27 is directly connected, vif30
O> * 140.1.1.0/25 [110/2] via 192.168.1.1, vif2, 00:13:44
O> * 140.1.1.128/25 [110/2] via 192.168.1.1, vif2, 00:13:44
O    141.108.10.0/30 [110/1] is directly connected, vif8, 00:12:12
C> * 141.108.10.0/30 is directly connected, vif8
```

```
O    192.168.1.0/30 [110/1] is directly connected, vif2, 00:13:54
C> * 192.168.1.0/30 is directly connected, vif2
R2#
```

| | |
|---|---|
| | **Note**<br>Note that R2 has access to the remote networks in area 0 or on the backbone, but not vice versa, because Router R2 is connected to area 2. |

Area 2 is not partitioned from the backbone. In fact, area 2 is directly connected to the backbone through Router R4.

Area 1 is not directly connected to the backbone. Therefore, Router R1 is missing IP networks.

The golden rule in any OSPF network is that all areas must be contiguous or all areas must be connected to the backbone. Scenario 2 includes three areas. If an area cannot be assigned to the backbone or is partitioned from the backbone, a virtual link is required. When designing a network, you use a virtual link to attach areas that do not have a physical connection to the backbone or in cases in which the backbone is partitioned, as in the example shown in *Figure 51*, page *600.*

*Figure 52*, below, displays the areas and the requirement for a virtual link.

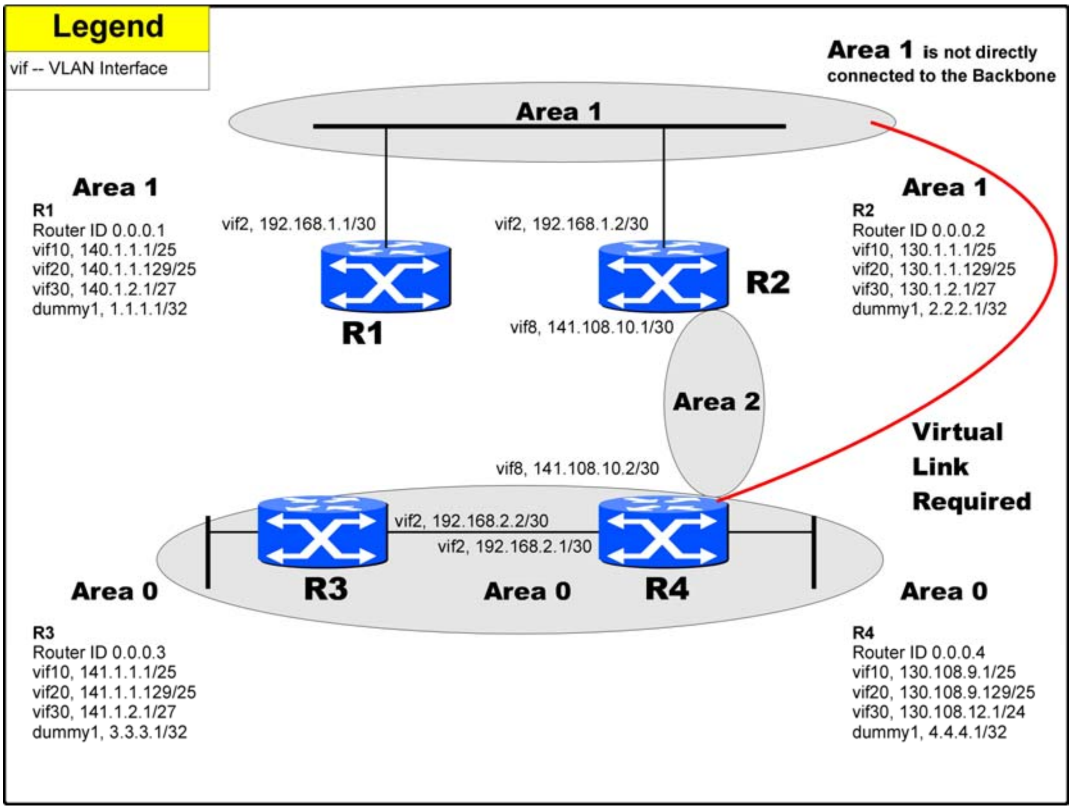



**Figure 52: Area Assignments and the Virtual Link Requirement**

The virtual link in this scenario is required from R2 to R4. The virtual link allows information about area 1 to be sent to the backbone. Another solution to this problem is to change the area 1 assignment to area 2 or to connect a physical link from area 1 to the backbone.

In this scenario, configure a virtual link between R2 and R4.

To create a virtual link, you use the following command:

```
R4(config)# router ospf 4
R4(config-router)# area 2 virtual-link 0.0.0.2
```

[**no**] **area** *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [[**authentication-key** *key*] | [**message-digest-key** *keyid* **md5** *key*]]

As can be seen, this command has several options. The following is a simplification:
**area** *area-id* **virtual-link** *router-id*
The *area-id* is the transit network between the two partitioned areas, in this case area 2. You can find the *router-id* by using the **show ip ospf database** command, which displays the complete OSPF database. Example 15 shows you how to discover the router IDs on R2 and R4.

Note that the extensive amount of information typically supplied by the **show ip ospf database** command is not all displayed in Example 15.

***Example 15: Show ip ospf database Command on R2 and R4***

```
R2>show ip ospf database
OSPF Router with ID (131.108.6.2) (Process ID 2)
R4>show ip ospf database
OSPF Router with ID (141.108.12.1) (Process ID 6)
```

You now have the information required to configure a virtual link between R3 and R4. Examples 17 and 18 display the configuration performed on Routers R2 and R4.

***Example 16: Configuring a Virtual Link on R2***

```
R2(config)#router ospf 2
R2(config-router)#area 2 virtual-link 0.0.0.2
```

***Example 17: Configuring a Virtual Link on R4***

```
R4(config)# router ospf  4
R4(config-router)#area 2 virtual-link 0.0.0.2
```

Use the **show ip ospf virtual-links** command on R2, demonstrated in Example 18, to ensure that the virtual link is active.

***Example 18: Show ip ospf virtual-links***

```
R4# show ip  ospf  virtual-links
Virtual Link VLINK0 to router 0.0.0.2 is up
  Transit area 0.0.0.2 via interface vif8
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adajcency state Full
```

Example 18 displays an active link to the remote OSPF router with the ID 141.108.12.1. Now, view the routing tables on R3 to determine whether the area 1 networks have been inserted into the IP routing table, as demonstrated in Example 19.

***Example 19: Show ip route on R3***

```
R3# show ip route
multipath equal cost limit: 1
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info

O> * 1.1.1.1/32 [110/13] via 192.168.2.1, vif2, 00:00:22
O    3.3.3.1/32 [110/10] is directly connected, dummy1, 02:05:31
C> * 3.3.3.1/32 is directly connected, dummy1
O> * 4.4.4.1/32 [110/11] via 192.168.2.1, vif2, 00:00:58
O> * 130.1.1.128/25 [110/3] via 192.168.2.1, vif2, 00:00:22
O> * 130.1.2.0/27 [110/3] via 192.168.2.1, vif2, 00:00:22
O> * 130.108.9.0/25 [110/2] via 192.168.2.1, vif2, 00:00:58
O> * 130.108.9.128/25 [110/2] via 192.168.2.1, vif2, 00:00:58
O> * 130.108.12.0/24 [110/2] via 192.168.2.1, vif2, 00:00:58
O> * 140.1.1.0/25 [110/4] via 192.168.2.1, vif2, 00:00:22
O> * 140.1.1.128/25 [110/4] via 192.168.2.1, vif2, 00:00:22
O    141.1.1.0/25 [110/1] is directly connected, vif10, 02:05:21
C> * 141.1.1.0/25 is directly connected, vif10
O    141.1.1.128/25 [110/1] is directly connected, vif20, 01:47:07
C> * 141.1.1.128/25 is directly connected, vif20
O    141.1.2.0/27 [110/1] is directly connected, vif30, 01:46:56
```

```
C> * 141.1.2.0/27 is directly connected, vif30
O> * 141.108.10.0/30 [110/2] via 192.168.2.1, vif2, 00:00:58
O> * 192.168.1.0/30 [110/3] via 192.168.2.1, vif2, 00:00:22
O    192.168.2.0/30 [110/1] is directly connected, vif2, 00:01:44
C> * 192.168.2.0/30 is directly connected, vif2
```

Router R3 discovers the remote networks from the partitioned area 1 through the virtual link between the routers R2 and R4 as demonstrated by the IP routing table in Example 19.

Examples 20, 21, and 22 show the three configurations of routers R2, R3, and R4, respectively. R1's configuration is unchanged from scenario 1.

***Example 20: Full Configuration on R2***

```
hostname R2
!
interface vlan vif2
 description *** Connection to R1 **
 tag 2
 ip 192.168.1.2/30
 ports 7
!
interface vlan vif8
 description *** Connection To R4 **
 tag 8
 ip 141.108.10.1/30
 ports 8
!
interface vlan vif10
 description *** Client Lan Connection **
 tag 10
 ip 130.1.1.1/25
 ports 1
!
interface vlan vif20
 description *** Client Lan Connection **
 tag 20
 ip 130.1.1.129/25
 ports 3
!
interface vlan vif30
 description *** Client Lan Connection **
 tag 30
 ip 130.1.2.1/27
 ports 5
 ip ospf network point-to-point
 ip ospf cost 1000
!
interface dummy dummy1
 ip 2.2.2.1/32
!
router ospf 2
 ospf router-id 0.0.0.2
 network 2.2.2.1/32 area 1
 network 130.1.1.0/25 area 1
 network 130.1.1.128/25 area 1
 network 130.1.2.0/27 area 1
 network 141.108.10.0/30 area 2
 network 192.168.1.0/30 area 1
 area 2 virtual-link 0.0.0.4
!
```

Example 21 displays R3's full configuration.

***Example 21: Full Configuration on R3***

```
hostname R3
!
interface vlan vif2
 description *** Connection to Router R4 **
 tag 2
 ip 192.168.2.2/30
 ports 24
!
interface vlan vif10
 tag 10
 ip 141.1.1.1/25
 ports 1
!
interface vlan vif20
 tag 20
 ip 141.1.1.129/25
 ports 3
!
interface vlan vif30
 tag 30
 ip 141.1.2.1/27
 ports 5
!
interface dummy dummy1
 ip 3.3.3.1/32
!
router ospf 3
 ospf router-id 0.0.0.3
 network 3.3.3.1/32 area 0
 network 141.1.1.0/25 area 0
 network 141.1.1.128/25 area 0
 network 141.1.2.0/27 area 0
 network 192.168.2.0/30 area 0
!
R3#
```

Example 22 displays R4's full configuration.

***Example 22: Full Configuration on R4***

```
Building configuration...

Current configuration:
! version 2_0_10
!
hostname R4
!
interface vlan vif2
 description *** Connection To R3 **
 tag 2
 ip 192.168.2.1/30
 ports 8
!
interface vlan vif8
 description *** Connection to Router R2 **
 tag 8
 ip 141.108.10.2/30
 ports 7
!
interface vlan vif10
 description *** Client Lan Connection **
 tag 10
```

```
 ip 130.108.9.1/25
 ports 1
!
interface vlan vif20
 tag 20
 ip 130.108.9.129/25
 ports 3
!
interface vlan vif30
 ip 130.108.12.1/24
 ports 5
!
interface dummy dummy1
 ip 4.4.4.1/32
!
router ospf 4
 ospf router-id 0.0.0.4
 network 4.4.4.1/32 area 0
 network 130.108.9.0/25 area 0
 network 130.108.9.128/25 area 0
 network 130.108.12.0/24 area 0
 network 141.108.10.0/30 area 2
 network 192.168.2.0/30 area 0
 area 2 virtual-link 0.0.0.2
!
```

Now, you move on to learn about some common OSPF commands you can use to ensure that remote networks are reachable.

### *Scenario 3: How OSPF Monitors, Manages, and Maintains Routes*

In this scenario, you re-examine in detail the network in *Figure 51*, page *600*, and discover some of the common OSPF commands for monitoring, managing, and maintaining IP routing tables. This scenario also looks at ways to configure OSPF to modify IP routing table entries, such as cost metrics and DR/BDR election.

*Table 24*, below, displays a summary of the commands executed in this scenario.

**Table 24: OSPF Commands for Monitoring, Managing, and Maintaining IP Routing Tables**

| Command | Description |
|---|---|
| **`show ip ospf`** | Displays the OSPF process and details such as OSPF process ID and router ID. |
| **`show ip ospf database`** | Displays routers topological database. |
| **`show ip ospf neighbor`** | Displays OSPF neighbors. |
| **`show ip ospf neighbor detail`** | Displays OSPF neighbors in detail, providing parameters, such as neighbor address, hello interval, and dead interval. |
| **`show ip ospf interface`** | Displays information on how OSPF has been configured for a given interface. |
| **`ip ospf priority`** | Interface command used to change the DR/BDR election process. |
| **`ip ospf cost`** | Interface command used to change the cost of an OSPF interface. |

Example 23 shows the output of the command **`show ip ospf`** taken from the backbone Router R3 in *Figure 51*, page *600*. *Table 25*, page *608*, explains how to read the most important information contained within the output.

Scenario 2, and thus this scenario, has four routers with the following router IDs:

- R1— 0.0.0.1
- R2— 0.0.0.2
- R3— 0.0.0.3

• R4— 0.0.0.4

This information is shown in the examples that follow.

***Example 23:  Show ip ospf Output***

```
R3#  show ip ospf
 OSPF Routing Process 3, Router ID: 0.0.0.3
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 MTU_ignored flag is disabled
 Opaque-LSA capability is on
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0. Checksum Sum 0x0
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Traffic-Engineering advertisement: disabled
 Cspf calculation: disabled
 Number of areas attached to this router: 1

 Area ID: 0.0.0.0 (Backbone)
   Number of interfaces in this area: Total: 5, Active: 5
   Number of fully adjacent neighbors in this area: 1
   Area has no authentication
   SPF algorithm executed 12 times
   Number of LSA 14. Checksum Sum 0x75a87
```

**Table 25:  Explanation of the show ip ospf Command Output Taken from R3**

| Field | Explanation |
|---|---|
| OSPF process Id | Displays the process ID.. |
| OSPF router Id | Displays the router id in this process |
| Minimum LSA interval 5 | The amount of time that the Master-OS™ waits before the SPF |
| secs Minimum LSA arrival 1 sec | calculation is completed after receiving an update. The minimum LSA interval is five seconds and the minimum LSA arrival is one second on R3. |
| Number of areas in this router is 1 | Displays the number of areas configured on the local router. In this example, R3 has all interfaces in the backbone, or area 0. So only one area is displayed by this command. |
| Area BACKBONE(0) | Displays the area the router is configured for. R3 is a backbone router, so this output advises the area in backbone 0. |
| Number of interfaces in this area is  5 | Displays the number of interfaces in area 0. R3 has  five interfaces in area 0 (including the dummy interface). |
| Area has no authentication | Displays the fact that no authentication is used on R3. |

Example 24 shows the output of the command show ip ospf database taken from the backbone R3 in *Figure 51*, page *600*. *Table 26*, page *609* explains how to read the most important information contained within the output.

***Example 24:  Show ip ospf database Output***

```
R3# show  ip ospf  database

       OSPF Router process 3 with ID (0.0.0.3)

                Router Link States (Area 0.0.0.0)
```

```
Link ID         ADV Router      Age  Seq#       CkSum  Link count
0.0.0.2         0.0.0.2          372 0x80000005 0xa995 1
0.0.0.3         0.0.0.3         1324 0x8000000b 0x36c9 5
0.0.0.4         0.0.0.4          368 0x8000000e 0x1754 5

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.2.1     0.0.0.4         1795 0x80000001 0xd70e

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
1.1.1.1         0.0.0.2          458 0x80000001 0x9fac 1.1.1.1/32
2.2.2.1         0.0.0.2          458 0x80000001 0x71d8 2.2.2.1/32
130.1.1.0       0.0.0.2          458 0x80000001 0xb4a0 130.1.1.0/25
130.1.1.128     0.0.0.2          458 0x80000001 0xaf25 130.1.1.128/25
140.1.1.0       0.0.0.2          458 0x80000001 0x3c0e 140.1.1.0/25
140.1.1.128     0.0.0.2          458 0x80000001 0x3792 140.1.1.128/25
140.1.2.0       0.0.0.2          458 0x80000001 0x7375 140.1.2.0/27
141.108.10.0    0.0.0.2          458 0x80000001 0xa3b5 141.108.10.0/30
141.108.10.0    0.0.0.4          936 0x80000001 0xf15c 141.108.10.0/30
192.168.1.0     0.0.0.2          458 0x80000001 0x9a58 192.168.1.0/30
```

**Table 26: Explanation of the `show ip ospf database` Command**

| Field | Explanation |
|---|---|
| OSPF Router with ID (0.0.0.3) (Process ID 3) | The router ID and process ID on the router configured by the network administrator. |
| Router Link States (Area 0) | Displays the link-state advertisements from connected neighbors discovered by the Hello protocol. |
| Summary Net Link States (Area 0) | Information displayed by ABRs. |

To show you some different output, look at two more examples from Scenario 2: one from R2 and one from R4. Example 25 displays the **`show ip ospf neighbor`** command from R2.

***Example 25: Show ip ospf neighbor from R2***

```
R2# show ip ospf neighbor

OSPF process 2:
Neighbor ID     Pri   State           Dead Time    Address         Interface        RXmtL
RqstL DBsmL
0.0.0.4           1   Full/Backup     00:00:36     141.108.10.2    vif8:141.108.10.1  0
0     0
0.0.0.1           1   Full/DR         00:00:30     192.168.1.1     vif2:192.168.1.2   0
0     0
0.0.0.4           1   Full/ -         00:00:39     141.108.10.2    VLINK     0        0
0     0
R2#
```

Router R2 has two neighbors: one across the Ethernet segment and another through the virtual link to R4. The **`show ip ospf neighbor`** command displays the neighbor router ID and the priority of the neighbor (both 1 in this example) as well as the DR. Notice that the DR is R1 as seen by R2. The state of the adjacency (Full) and the dead time are displayed. The dead time is the amount of time before the adjacency is declared dead or inactive if a Hello packet is not received. The dead time must be the same of the adjacent router. **It is advised that you configure the dead time to be four times the hello interval.** The address field displays the remote router's IP address. In this case, the IP address assigned to R1 is  The interface field describes the outbound interface from which the neighbor was discovered. Example 26 displays the neighbors on R4 in more detail by adding the **`detail`** parameter to the **`show ip ospf neighbor`** command.

### *Example 26: Show ip ospf neighbor detail from R4*

```
R4# show  ip  ospf  neighbor detail
 Neighbor 0.0.0.2, interface address 141.108.10.1
    In the area 0.0.0.2 via interface vif8
    Neighbor is dynamic (neighbor was learned via broadcast messages)
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 141.108.10.1, BDR is 141.108.10.2
    Options is 0x42 (*|O|-|-|-|-|E|-)
    Dead timer due in 00:00:34
    Neighbor is up for 00:18:26
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on

 Neighbor 0.0.0.3, interface address 192.168.2.2
    In the area 0.0.0.0 via interface vif2
    Neighbor is dynamic (neighbor was learned via broadcast messages)
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 192.168.2.1, BDR is 192.168.2.2
    Options is 0x42 (*|O|-|-|-|-|E|-)
    Dead timer due in 00:00:35
    Neighbor is up for 00:33:27
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on
```

Router R4 has no adjacency across any broadcast media, such as Ethernet.

Therefore, the neighbors are all in a Full state but no DR or BDR is selected across the wide-area network (WAN) link, because the WAN link is considered a point-to-point link. To determine what type of OSPF network the given interface is, use the **`show ip ospf interface`** command. Example 27 displays this command in its most basic form taken from R4. You can provide more parameters, such as **interface vif** *number***.**

### *Example 27: Show ip ospf interface from R4*

```
R4# show ip ospf interface
  [INTERFACE]  Interface name
  |            Output modifiers
R4# show ip ospf interface
eth0 is down, line protocol is down
  OSPF not enabled on this interface
dummy0 is down, line protocol is down
  OSPF not enabled on this interface
vif2 is up, line protocol is up
  Internet Address 192.168.2.1/30, Area 0.0.0.0
    Router ID 0.0.0.4, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 0.0.0.4, Interface Address 192.168.2.1
    Backup Designated Router (ID) 0.0.0.3, Interface Address 192.168.2.2
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:09
    Neighbor Count is 1, Adjacent neighbor count is 1
    Crypt Sequence Number is 0
dummy1 is up, line protocol is up
  Internet Address 4.4.4.1/32, Area 0.0.0.0
    Router ID 0.0.0.4, Network Type BROADCAST, Cost: 10
```

```
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 0.0.0.4, Interface Address 4.4.4.1
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:02
    Neighbor Count is 0, Adjacent neighbor count is 0
    Crypt Sequence Number is 0
vif10 is up, line protocol is up
  Internet Address 130.108.9.1/25, Area 0.0.0.0
    Router ID 0.0.0.4, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 0.0.0.4, Interface Address 130.108.9.1
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:07
    Neighbor Count is 0, Adjacent neighbor count is 0
    Crypt Sequence Number is 0
vif20 is up, line protocol is up
  Internet Address 130.108.9.129/25, Area 0.0.0.0
    Router ID 0.0.0.4, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 0.0.0.4, Interface Address 130.108.9.129
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:07
    Neighbor Count is 0, Adjacent neighbor count is 0
    Crypt Sequence Number is 0
vif30 is down, line protocol is down
  OSPF not enabled on this interface
vif8 is up, line protocol is up
  Internet Address 141.108.10.2/30, Area 0.0.0.2
    Router ID 0.0.0.4, Network Type BROADCAST, Cost: 10
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 0.0.0.2, Interface Address 141.108.10.1
    Backup Designated Router (ID) 0.0.0.4, Interface Address 141.108.10.2
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:02
    Neighbor Count is 1, Adjacent neighbor count is 1
    Crypt Sequence Number is 0
 R4#
```

Router R4 has six interfaces configured with OSPF, so you should expect details about those interfaces. Example 27 displays all interface network types as BROADCAST. Note that because R4 has no neighbors over the Ethernet network, no DR/BDR is elected, because there is no need. The dead interval is four times the hello interval on all interfaces.

Now use some interface commands on the *Figure 51*, page *600*, network to modify the behavior of the DR/BDR election process. Start by changing the designated router in area 1 and ensure that Router R2 becomes the DR. Example 28 displays the current DR and the configuration change on R2 to make the priority higher than R1 by setting the priority to 255.

***Example 28: Changing the IP OSPF Priority on R2***

```
R2# show ip ospf neighbor

OSPF process 2:
Neighbor ID      Pri   State            Dead Time    Address          Interface
      RXmtL RqstL DBsmL
0.0.0.4           1    Full/Backup      00:00:36     141.108.10.2     vif8:141.108.1 0.1      0
0     0
0.0.0.1           1    Full/DR          00:00:30     192.168.1.1      vif2:192.168.1.2        0
0     0
0.0.0.4           1    Full/ -          00:00:39     141.108.10.2     VLINK0                  0
0     0
```

```
R2(config)# interface  vif2
R2(config-vif2)# ip  ospf  priority 255

R2#  show  ip ospf  neighbor

OSPF process 2:
Neighbor ID     Pri   State           Dead Time   Address         Interface
      RXmtL RqstL DBsmL
0.0.0.4           1   Full/Backup     00:00:30    141.108.10.2    vif8:141.108.10.1     0
0     0
0.0.0.1           1   Full/DR         00:00:34    192.168.1.1     vif2:192.168.1.2     0
0     0
0.0.0.4           1   Full/ -         00:00:33    141.108.10.2    VLINK0               0
0     0

R2# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address
Interface
131.108.5.1 1 FULL/DR 00:00:31 131.108.1.1
141.108.12.1 1 FULL/ - 00:00:32 141.108.10.2
```

Example 28 stills displays the DR as R1 and not R2 even after the configuration setting changes the priority to 255, because the election process has already taken place and R1 is still the DR. Example 29 displays the neighbor state as seen by R2, which is now the backup designated router (BDR).

***Example 29: Show ip ospf neighbor on R2***

```
R2#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address
Interface
131.108.5.1 1 FULL/BDR 00:00:34 131.108.1.1
141.108.12.1 1 FULL/ - 00:00:35 141.108.10.2
```

The final command in this scenario is the **`ip ospf cost`** command. You use this command to change the cost OS900s assign by default by using the formula OSPF cost = $10^8$ / bandwidth. This command is not the only method you can use to change the cost. You can also use the **`bandwidth`** command on a particular interface and let the Master-OS™ use the bandwidth portion of the cost formula to calculate the new cost.

**Note**

You can also use the command **auto-cost reference-bandwidth** *referencebandwidth* during the OSPF process to change the bandwidth portion of the cost calculation. You should set this command equally across all your routers if you choose to use it. The *reference-bandwidth* is set to $10^8$ by default.

**Table 27: Summary of OS™ Commands used in this Section**

| Command | Purpose |
|---|---|
| **`show ip route ospf`** | Displays IP routing tables. |
| **`router ospf <0-65535>`**<br>where,<br>`<0-65535>`: OSPF process ID. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value. | Enables OSPF routing. The process ID is local to the router. You can have more than one OSPF running. |
| **`network A.B.C.D/M area <0-4294967295>`**<br>where,<br>`A.B.C.D/M`: A.B.C.D/M OSPF network prefix. (You can use the mask to use a single command to define one or more multiple interfaces to be associated with a specific OSPF area. The area ID can be a decimal value or an IP address.) | Enables network advertisements out of a particular interface and also the routing of the same interface through OSPF. |
| **`show ip ospf`** | Displays the OSPF process and details, such as OSPF process ID and router ID. |
| **`show ip ospf database`** | Displays router's topological database. |
| **`show ip ospf neighbor`** | Displays OSPF neighbors. |
| **`show ip ospf neighbor detail`** | Displays OSPF neighbors in detail, providing such parameters as neighbor address, hello interval, and dead interval. |
| **`show ip ospf interface`** | Displays information on how OSPF has been configured for a given interface. |
| **`interface vlan IFNAME`**<br>where,<br>`IFNAME`: Interface ID having the format `vifX`, where `X` is a decimal number in the range 1-4095. | In configuration mode, enables you modify an interface number, |
| **`ip ospf cost <1-65535>`**<br>where,<br>`<1-65535>`: Cost | Interface command that changes the cost of an OSPF interface. |
| **`ip ospf priority <0-255>`**<br>where,<br>`<0-255>`: IP OSPF priority. Default: 1. | Interface command that changes the DR/BDR election process. |
| **`ip ospf network (broadcast\|non-broadcast\|point-to-multipoint\|point-to-point)`** | Interface command that changes the network type. |
| **`show ip protocols`** | Displays all routing protocols in use on a OS900. |
| **`hostname WORD`**<br>where,<br>`WORD`: OS900's network name. | Configures a name on a router. |

## Border Gateway Protocol (BGP)

### General

The Border Gateway Protocol (BGP) is a routing protocol whose primary function is to designate reachability *within* and *between* **autonomous systems**[75]. This function is performed by exchanging routing information between routers in the network of autonomous systems. The information is sufficient to construct a graph of AS connectivity from which routing loops can be opened and some policy decisions at the AS level can be enforced. To characterize the set of policy decisions that can be enforced using BGP, the rule that a BGP operating system advertise to its peers in neighboring ASs only those routes that it itself uses has to be applied. This rule reflects the "hop-by-hop" routing paradigm generally used throughout the current Internet. Note that some policies cannot be supported by the "hop-by-hop" routing paradigm and thus require techniques such as source routing to enforce them. For example, BGP does not enable one AS to send traffic to a neighboring AS intending that the traffic take a different route from that taken by traffic originating in the neighboring AS. On the other hand, BGP can support any policy conforming to the "hop-by-hop" routing paradigm. Since the current Internet uses only the "hop-by-hop" routing paradigm and since BGP can support any policy that conforms to that paradigm, BGP is highly applicable as an inter-AS routing protocol for the current internet as well as for very large private IP networks.

BGP runs over the reliable transport protocol TCP. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. Any authentication scheme used by the transport protocol may be used in addition to BGP's own authentication mechanisms. The error notification mechanism used in BGP assumes that the transport protocol supports a "graceful" close, i.e., that all outstanding data will be delivered before the connection is closed.

TCP meets BGP's transport requirements and is present in virtually all commercial routers and hosts. In the following descriptions, the phrase "transport protocol connection" can be understood to refer to a TCP connection. BGP uses TCP port 179 for establishing its connections.

Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when a host has detected a change. Only the affected part of the routing table is sent.

The OS900 implements BGP-4, the latest BGP version. BGP-4 lets adminstrators configure cost metrics based on policy statements.

The routers inside the autonomous network maintain two routing tables; one for IBGP and one for EBGP.

BGP-4 makes it easy to use Classless Inter-Domain Routing (CIDR), which is a way to have more addresses within the network than with the current IP address assignment scheme.

### Configuration

To configure an OS900 to operate with BGP:

1. Enter **`configure terminal`** mode.
2. Configure VLAN interfaces with IP addresses to enable router-to-router and router-to-networks communication.
   (The procedure for configuring VLAN interfaces is given in ***Chapter 7:*** *Interfaces*, page *181*.)
3. Assign a BGP ID to the OS900 by invoking the command:
   **`router bgp <1-65535>`**
   where,

[75] An Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASs. Since this definition, it has become common for a single AS to use several interior gateway protocols and sometimes several sets of metrics within an AS. The use of the term Autonomous System here stresses the fact that, even when multiple IBGPs and metrics are used, the administration of an AS appears to other ASs to have a single coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

**<1-65535>**: Range of BGP Router IDs for the OS900 from which one is to be selected.

4. Assign a BGP ID to each neighbor router by invoking the command:
   **`neighbor A.B.C.D remote-as <1-65535>`**
   where,
   **A.B.C.D**: Neighbor address
   **<1-65535>**: Range of BGP Router IDs of the neighbor from which one is to be selected.
5. Assign a BGP ID to each neighbor router by invoking the command:
   **`neighbor A.B.C.D remote-as <1-65535>`**
   where,
   **A.B.C.D**: Neighbor address
   **<1-65535>**: Range of BGP Router IDs of the neighbor from which one is to be selected.
6. To configure an OS900 as the next hop for a BGP-speaking neighbor or peer group, disable the next hop calculation by invoking the command:
   **`neighbor A.B.C.D next-hop-self`**
   where,
   **A.B.C.D**: Neighbor address
   The above command is useful in non-mesh networks where BGP neighbors might not have direct access to other neighbors on the same IP subnet.
7. Specify the IP addresses of the OS900 interfaces connected to networks by repeatedly invoking the command:
   **`network A.B.C.D/M`**
   where,
   **A.B.C.D/M**: Interface IP address

**Example**

Following is an example in which the primary function of BGP is designated, namely, reachability between and within Autonomous systems.

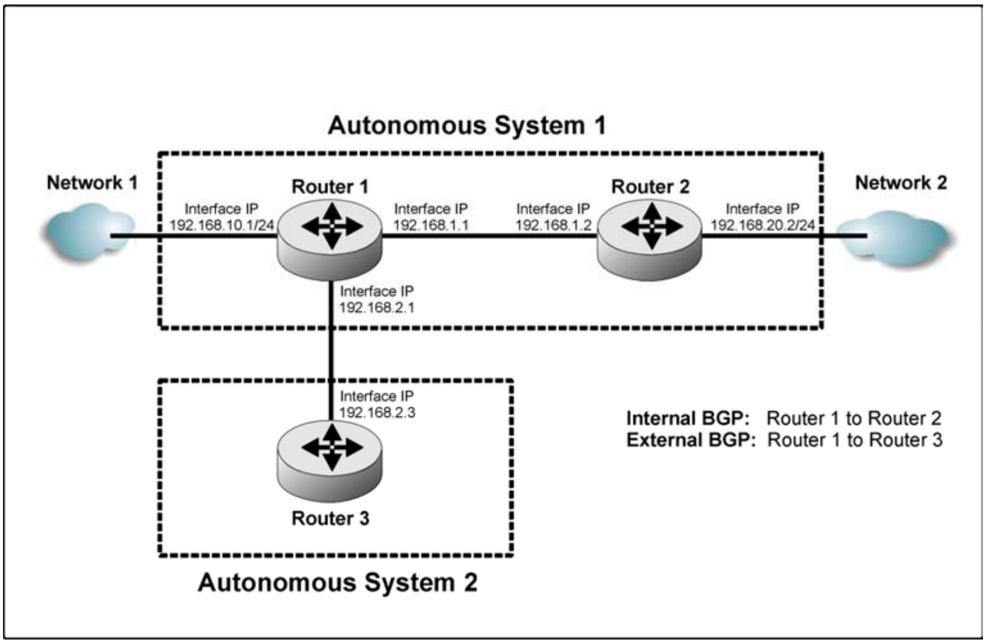



**Figure 53: Network on which BGP is Configured**

Router 1

```
OS900> enable
OS900# configure terminal

OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 7
OS900(config-vif1)# tag 3007
Interface is activated.
OS900(config-vif1)# name R1_to_R2
OS900(config-vif1)# ip 192.168.1.1/24
OS900(config-if)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 6
OS900(config-vif2)# tag 3006
Interface is activated.
OS900(config-vif2)# name R1_to_R3
OS900(config-vif2)# ip 192.168.2.1/24
OS900(config-if)# exit

OS900(config)# interface vlan vif3
OS900(config-vif3)# ports 5
OS900(config-vif3)# tag 3005
Interface is activated.
OS900(config-vif3)# ip 192.168.10.1/24
OS900(config-if)# exit

OS900(config)# router bgp 100
OS900(config-router)# neighbor 192.168.1.2 remote-as 100
OS900(config-router)# neighbor 192.168.1.2 next-hop-self
OS900(config-router)# network 192.168.10.0/24
OS900(config-router)# neighbor 192.168.2.3 remote-as 300
OS900(config-router)#
```

Router 2

```
OS900> enable
OS900# configure terminal

OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 8
OS900(config-vif1)# tag 3008
Interface is activated.
OS900(config-vif1)# name R2_to_R1
OS900(config-vif1)# ip 192.168.1.2/24
OS900(config-if)# exit

OS900(config)# interface vlan vif2
OS900(config-vif2)# ports 6
OS900(config-vif2)# tag 3006
Interface is activated.
OS900(config-vif2)# name R2_to_Net2
OS900(config-vif2)# ip 192.168.20.2/24
OS900(config-if)# exit

OS900(config)# router bgp 100
OS900(config-router)# neighbor 192.168.1.1 remote-as 100
OS900(config-router)# network 192.168.20.0/24
OS900(config-router)#
```

| | **Note** |
|---|---|
| | The "router bgp" ID between two routers in the same Autonomous System (AS) must be the same. This example shows the router bgp ID as 100 between the two routers in the same AS. |

Router 3

```
OS900> enable
OS900# configure terminal

OS900(config)# interface vlan vif1
OS900(config-vif1)# ports 8
OS900(config-vif1)# tag 3008
Interface is activated.
OS900(config-vif1)# name R3_to_R1
OS900(config-vif1)# ip 192.168.2.3/24
OS900(config-if)# exit

OS900(config)# router bgp 300
OS900(config-router)# neighbor 192.168.2.1 remote-as 100
OS900(config-router)#
```

| | **Note** |
|---|---|
| | The OS900 sends syslog messages on BGP state machine transitions to `"Established" or "Idle" states.`<br>Example<br>`2003/05/19 07:27:15 BGP : 172.28.2.2 [FSM] Hold_Timer_expired (Established->Idle)`<br>`2003/05/19 07:29:20 BGP : 172.28.2.2 [FSM] Receive_KEEPALIVE_message (OpenConfirm->Established)` |

## Virtual Router Redundancy Protocol (VRRP)

### Definition

VRRP (RFC 2338) is a protocol that is used to eliminate the problem of single-point-of-failure resulting from the failure of a statically configured gateway/router by configuring two or more routers on a network to operate in mutual redundancy mode.

### Principle of Operation

VRRP dynamically assigns responsibility to one router (Master Router) in a network to route packets sent from the hosts in the network. The other routers in the network serve as Backup Routers and have differing takeover priorities. VRRP routers periodically send VRRP advertisement messages using IP multicast datagrams. A Backup Router preempts (takes over the routing responsibility from) the Master Router only if it currently has a higher priority or if the Master Router does not advertise within a pre-defined time interval.

If a router's UNI link[76] fails, traffic meant to go via the router will now go via another.

### Configuration

To configure VRRP on an OS900:

1. For convenience, change the host name of the OS900 to a unique name by invoking the command:

   **`hostname WORD`**

   where,

   **`WORD`**: OS900's host name

[76] The link between the user device (e.g., switch) and router – see *Figure 54*, page *619*.

2. Create a VLAN interface via which the OS900 is to run VRRP, and assign an IP address to it. (The procedure for creating VLAN interfaces is described in ***Chapter 7:*** *Interfaces*, page *177*.)
3. In the VLAN interface mode, enter `VRRP` mode by invoking the command:

   **vrrp**
4. Enable VRRP on the VLAN interface by invoking the command:

   **enable**
5. Set up one (or more) virtual router(s)[77] with virtual router IP(s) on the VLAN interface by (repeatedly) invoking the commands in steps *5.1* to *0* below:

   5.1. Create a Virtual Router on the VLAN interface by invoking the command:

   **virtual-router <1-255>**

   where,

   **<1-255>**: Range of IDs for virtual routers.

   5.2. Assign an IP address to the Virtual Router by invoking the command:

   **virtual-ip a.b.c.d**

   where,

   **a.b.c.d**: IP address of virtual router.

   | | |
   |---|---|
   | | **Note**<br>If the OS900 is an Owner[78], Step *6* below will be ineffectual meaning that the OS900 cannot be set to switchover to another VRRP router (e.g., OS900) when its NNI link[79] fails! |

   5.3. Enable the Virtual Router on the VLAN interface by invoking the command:

   **enable**

   | | |
   |---|---|
   | | **Note**<br>Identical Virtual Routers must be set up on each physical router (using the commands in steps *5.1* to *0* above). |

6. (Optional) Enable a Non-Owner[80] OS900 to switch to the other OS900 when its NNI link breaks by invoking the command:

   **track-interface WORD**

   where,

   **WORD**: ID of the interface connected to NNI side of the OS900.

   To revoke this option, invoke the command: **no track-interface**.
7. (Optional) Set the tracking priority of a Non-Owner OS900 by invoking the command:

   **track-priority <1-254>|default**

   where,

   **<1-254>**: Range of tracking priorities for the OS900 from which one is to be selected. (The OS900 to which a higher priority is assigned will be the master.)

   **default**: Default tracking priority. **255** for Owner, **100** for Non-Owner.

Other configuration parameters (using CLI commands) are optional.

---

[77] Setting up as many virtual routers as the number of physical routers enables the VRRP to share the traffic load between the physical routers.

[78] An OS900 is an *Owner* of a Virtual Router if the IP address of the OS900's VLAN interface connected to the UNI link is assigned to the Virtual Router. The tracking priority of an Owner is 255 (highest) and fixed!

[79] The link between the router and Network – see *Figure 54*, page *619*.

[80] An OS900 is a *Non-Owner* of a Virtual Router if the IP address of the OS900's VLAN interface connected to the UNI link is *not* assigned to the Virtual Router. The tracking priority of a Non-Owner is user-settable to any value in the range **<1-254>** as shown in the next step!

### Example

***Network***

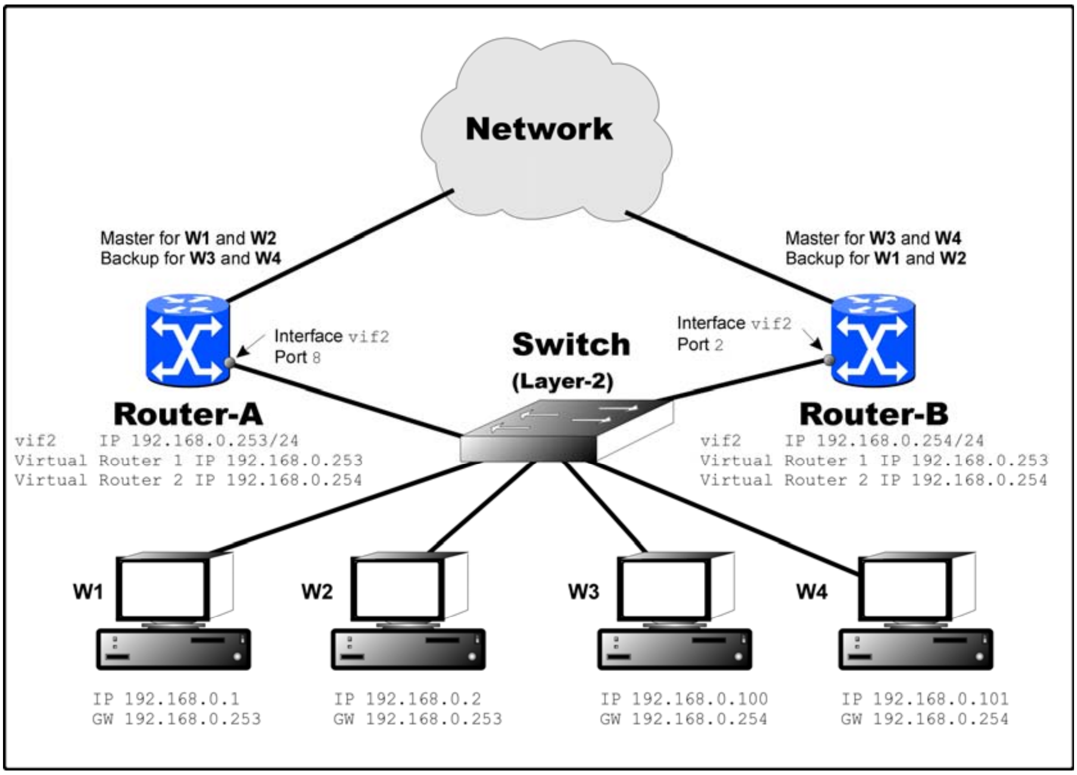



**Figure 54: Network on which VRRP is Configured**

*Figure 54*, above, is an example of a network to which VRRP can be applied.

Both Router-A (an OS900) and Router-B (an OS900) are attached to the same LAN (subnet), so that they can be configured to backup each other and also run in load-sharing mode when both routers are UP.

If the *UNI link* of Router-A fails, the VRRP makes Router-B take over and announce Router-A's IP address as its own. Traffic meant to go via Router-A will now go via Router-B and traffic meant to go via Router-B will continue to go via Router-B.

Similarly, if the *UNI link* of Router-B fails, the VRRP makes Router-A take over and announce Router-B's IP address as its own. Traffic meant to go via Router-B will now go via Router-A and traffic meant to go via Router-A will continue to go via Router-A.

*Two* virtual routers are configured to enable the VRRP to share the traffic load between the *two* physical routers (Router-A and Router-B).
Virtual Router 1 is the default gateway for W1 and W2 because its IP address is the same as the default gateway address of W1 and W2.
Virtual Router 2 is the default gateway for W3 and W4 because its IP address is the same as the default gateway address of W3 and W4.

Router-A is the Owner of Virtual Router 1. Accordingly, the priority of Router-A for the Virtual Router 1 is 255 (highest) and fixed! Router-A was made Owner in order to save on an IP address. But this saving prevents setting of Router-A to direct its traffic via Router-B in case its NNI link fails!

Router-B is the owner of Virtual Router 2 Accordingly, the priority of Router-B for the Virtual Router 2 is 255 (highest) and fixed! Router-B was made Owner in order to save on an IP address. But this saving prevents setting of Router-B to direct its traffic via Router-A in case its NNI link fails!

As required, *identical* virtual routers (i.e., having the same virtual router IDs – see command in Step *5.1*, page *618* – and same virtual IP addresses – see command in Step *5.2*, page *618*) are configured on the *two* physical routers.

The ID for the VLAN interfaces on both physical routers is set to **vif2**. Instead, different IDs could as well have been set.

The same tag is assigned to the VLAN interface on Router-A and on Router-B. Under this condition member ports of the VLAN interface on the routers can be all tagged, all untagged, or some tagged and others untagged. If different tags are assigned to the two interfaces, all ports must be untagged!

### *Configuration*

Following are the CLI commands for implementing the required VRRP configuration on Router-A and Router-B in the network shown in *Figure 54*, above.

### Router-A

```
----------Changing the Name of the first OS900 to Router-A----------

OS910(config)# hostname Router-A

----------------------Creating a VLAN interface----------------------

Router-A(config)# interface vlan vif2
Router-A(config-vif2)# ports 8
Router-A(config-vif2)# tag 10
Interface is activated.

------------Assigning an IP address to the VLAN interface------------

Router-A(config-vif2)# ip 192.168.0.253/24

-----------Creating a VRRP Interface on the VLAN interface-----------

Router-A(config-vif2)# vrrp
Created VRRP interface on device vif2

-----------------Enabling VRRP on the VLAN interface-----------------

Router-A(config-if-vrrp)# enable
VRRP on vif2 is enabled.

-------Creating the first Virtual Router on the VLAN interface-------

Router-A(config-if-vrrp)# virtual-router 1
Created virtual router 1 on device vif2

---------Assigning an IP address to the first Virtual Router---------

Router-A(config-if-vrrp-vr)# virtual-ip 192.168.0.253

-------Enabling the first Virtual Router on the VLAN interface-------

Router-A(config-if-vrrp-vr)# enable
Virtual router 1 on vif2 is enabled.
Router-A(config-if-vrrp-vr)# exit

------Creating the second Virtual Router on the VLAN interface------

Router-A(config-if-vrrp)# virtual-router 2
Created virtual router 2 on device vif2

--------Assigning an IP address to the second Virtual Router--------

Router-A(config-if-vrrp-vr)# virtual-ip 192.168.0.254

------Enabling the second Virtual Router on the VLAN interface------

Router-A(config-if-vrrp-vr)# enable
Virtual router 2 on vif2 is enabled.
Router-A(config-if-vrrp-vr)# exit
Router-A(config-if-vrrp)# exit
Router-A(config-vif2)# exit
Router-A(config)#
```

## Router-B

```
----------Changing the Name of the second OS900 to Router-B----------

OS910(config)# hostname Router-B

----------------------Creating a VLAN interface----------------------

Router-B(config)# interface vlan vif2
Router-B(config-vif2)# ports 2
Router-B(config-vif2)# tag 10
Interface is activated.

------------Assigning an IP address to the VLAN interface------------

Router-B(config-vif2)# ip 192.168.0.254/24

-----------Creating a VRRP Interface on the VLAN interface-----------

Router-B(config-vif2)# vrrp
Created VRRP interface on device vif2

-----------------Enabling VRRP on the VLAN interface-----------------

Router-B(config-if-vrrp)# enable
VRRP on vif2 is enabled.

-------Creating the first Virtual Router on the VLAN interface-------

Router-B(config-if-vrrp)# virtual-router 1
Created virtual router 1 on device vif2

---------Assigning an IP address to the first Virtual Router---------

Router-B(config-if-vrrp-vr)# virtual-ip 192.168.0.253
Router-B(config-if-vrrp-vr)#

-------Enabling the first Virtual Router on the VLAN interface-------

Router-B(config-if-vrrp-vr)# enable
Virtual router 1 on vif2 is enabled.
Router-B(config-if-vrrp-vr)# exit

------Creating the second Virtual Router on the VLAN interface------

Router-B(config-if-vrrp)# virtual-router 2
Created virtual router 2 on device vif2

--------Assigning an IP address to the second Virtual Router--------

Router-B(config-if-vrrp-vr)# virtual-ip 192.168.0.254

------Enabling the second Virtual Router on the VLAN interface------

Router-B(config-if-vrrp-vr)# enable
Virtual router 2 on vif2 is enabled.
Router-B(config-if-vrrp-vr)# exit
Router-B(config-if-vrrp)# exit
Router-B(config-vif2)# exit
Router-B(config)#
```

# Chapter 37: WDM Module

## Purpose

The WDM module is utilized to add or drop optical data carrier wavelengths.

## Application

To form (or participate in) WDM networks having point-to-point, multipoint, and ring topologies – see the section *Data paths in Networks of Various Topologies*, page *625*.

## Types

The following three types of WDM module are available:

***OADM*** Scalable, passive optical “add” and “drop” multiplexer/demultiplexer that can add and/or drop a specific channel (wavelength) to/from an optical WDM signal, while all other channels are routed from the input to the output with minimal attenuation. OADMs are required in ring and multipoint network topologies.

OADMs can be used to create a network topology in which a single wavelength can be added or dropped on demand, allowing an Optical Service Channel (OSC) to be provided at any point along a trunk. The technology enables flexible and intelligent planning and provisioning of optical services while at the same time simplifying deployment and maintenance of optical networks.

Dual-interface OADMs are available for building carrier networks protected by redundancy.

*Models* with 1 to 8 channels are available. The *modules* are passive and use optics only for their operation.

**EXP** ports IN and OUT carry only channels to be continued to the next OS900, and are used only in ring network topologies.

***Mux*** Multiplexes egress data coming over WDM channels[81] onto a single physical fiber. The module can multiplex up to 8 channels. The modules are passive and use optics only for their operation.

***Demux*** Demultiplexes ingress[82] data coming over WDM channels onto a single physical fiber. The multiplexer can demultiplex up to 8 channels. The modules are passive and use optics only for their operation.

[81] WDM channels carry data from one WDM unit (e.g., OS900, LambdaDriver) to another.

[82] Data entering the OS900.

# Layout

The layout of a WDM Module is shown in *Figure 55*, below.

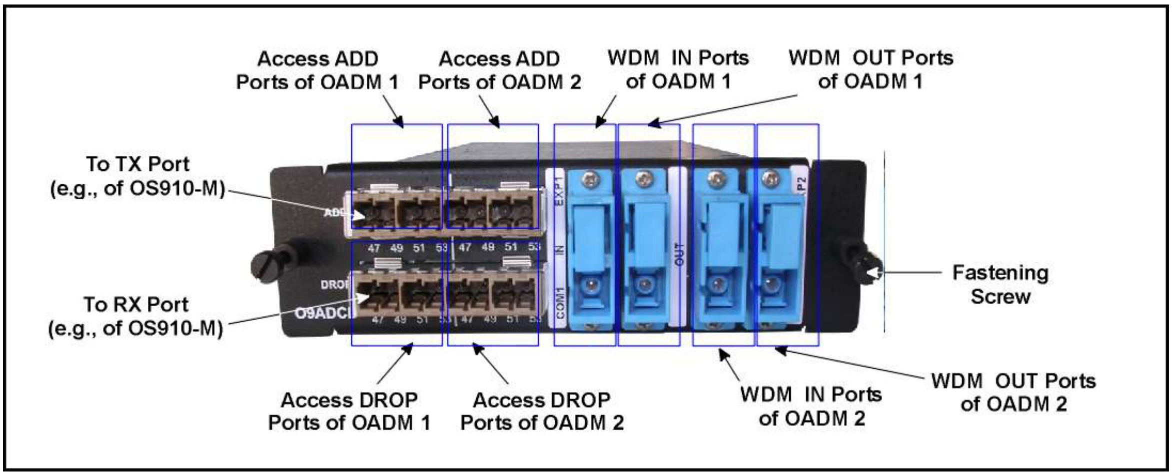



**Figure 55: WDM Module (Model 09ADCD) Layout**

# Mounting

WDM modules (up to two) can only be mounted in the OS910-M. To mount a WDM module:

1. Choose a receptacle[83] in the OS910-M into which the WDM module is to be inserted.
2. Holding the WDM module with the right side up, place the edges of the module's PCB between the left and right rails in the receptacle and slide it until its panel is level with the front panel of the OS910-M.
3. With a flat-head No.1 screwdriver, fasten the module with the two captive screws that are located on its edges.
4. With a philips screwdriver no. 1, fasten the module with the two captive screws that are located on its edges.

# Network Connection

The WDM module ports to be connected depend on the network configuration – see the section *Data paths in Networks of Various Topologies*, page *625*, below.

# Operation

The WDM Module is a plug-and-play passive device that does not require the user to set it into operation.

[83] Going from left to right across the front panel of the OS910-M model, the first receptacle (slot) for a service module is identified as number 2 and the second as number 3.

# Data paths in Networks of Various Topologies

## General

This appendix describes the data paths in networks of various topologies using OS910-Ms fitted with WDM modules.

## Point-to-Point Topology

The data flow through the WDM part of the network in point-to-point topology is shown in *Figure 56*, below.

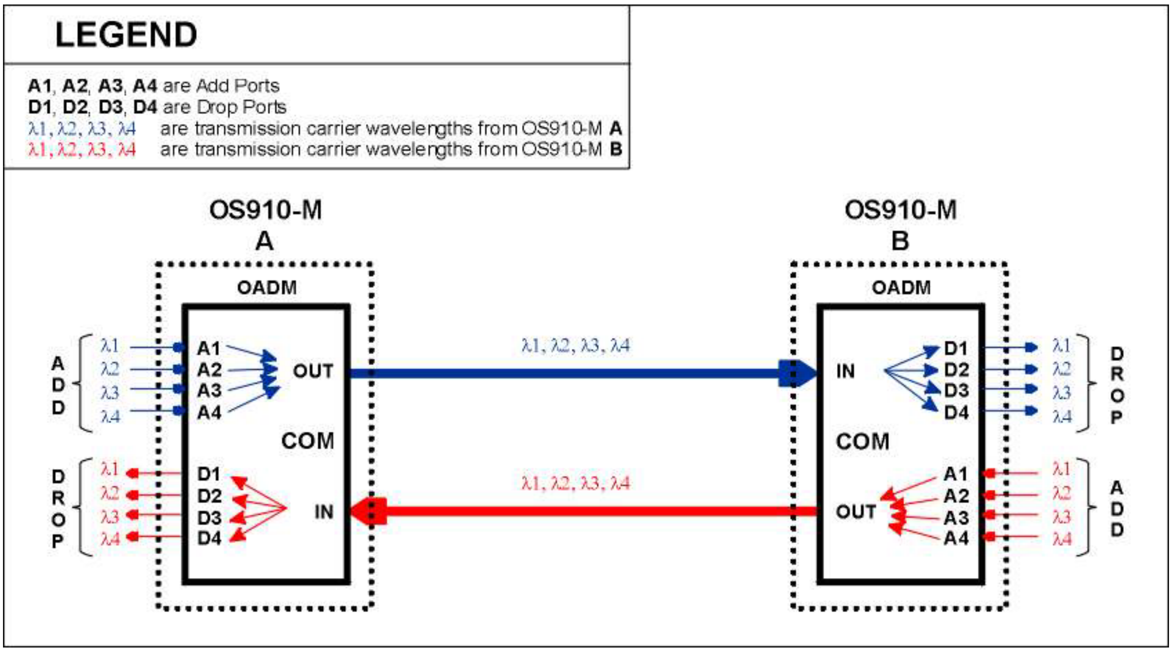



**Figure 56: Data Flow in a WDM Point-to-Point Topology**

## Multipoint Topology

The data flow through the WDM part of the network in multipoint topology is shown in *Figure 57*, below.

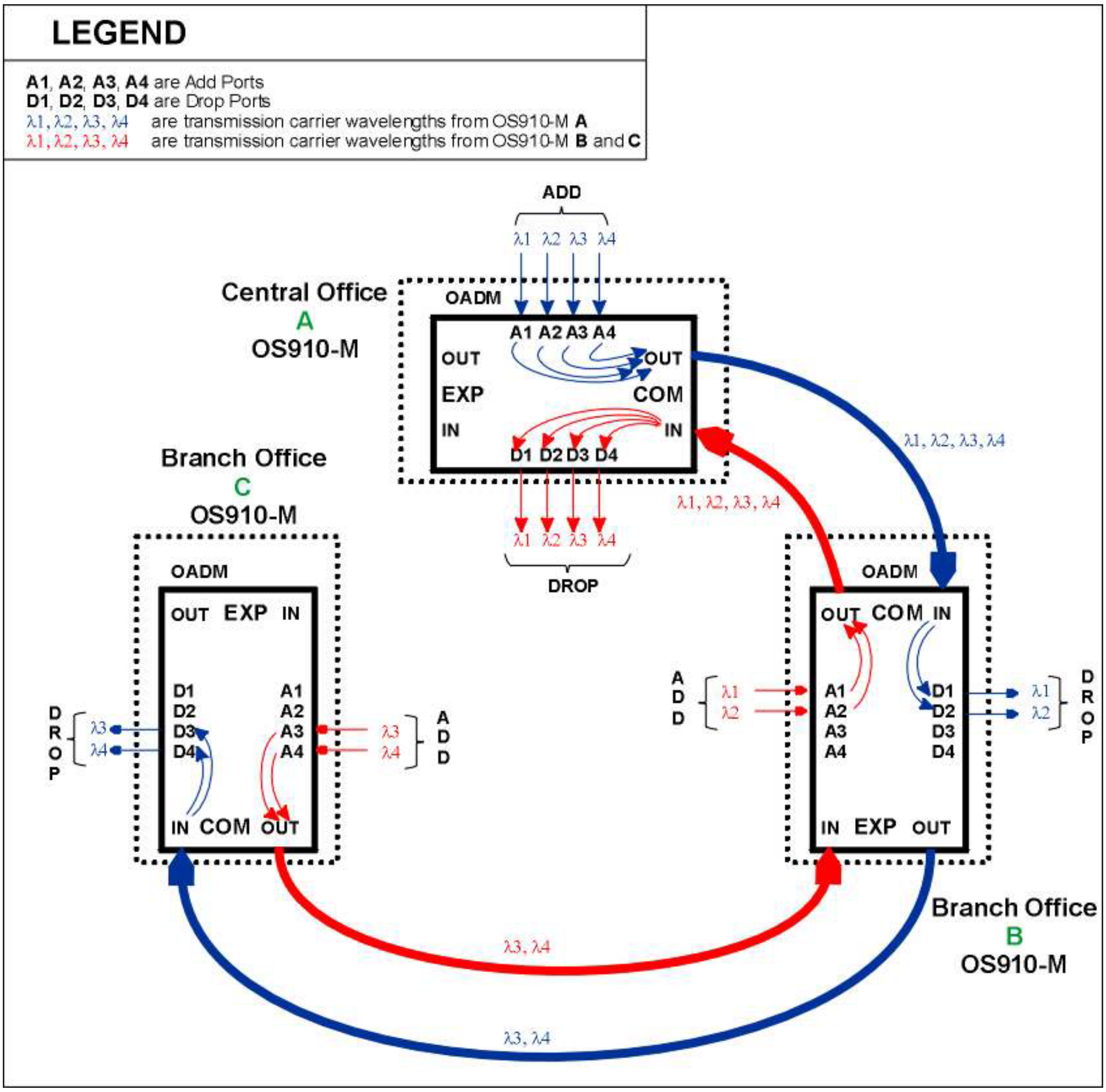



**Figure 57: Data Flow in a WDM Multipoint Topology**

## Ring Topology

The data flow through the WDM part of the network in ring topology is shown in *Figure 58*, below. The WDM module used is a dual-sided OADM module like that shown in *Figure 55*, page *624*. The connection of three long-haul fiber pairs instead of two provides fiber redundancy protection. This means that even if two of ***any*** of the long-haul fibers fail, the network will recover automatically within milliseconds and continue normal operation.

OS910-M **A** ports 1-4 are logically connected to OS910-M **B** ports 5-8. OS910-M **B** ports 1-4 are logically connected to OS910-M C ports 5-8. OS910-M **C** ports 1-4 are logically connected to OS910-M **A** ports 5-8.

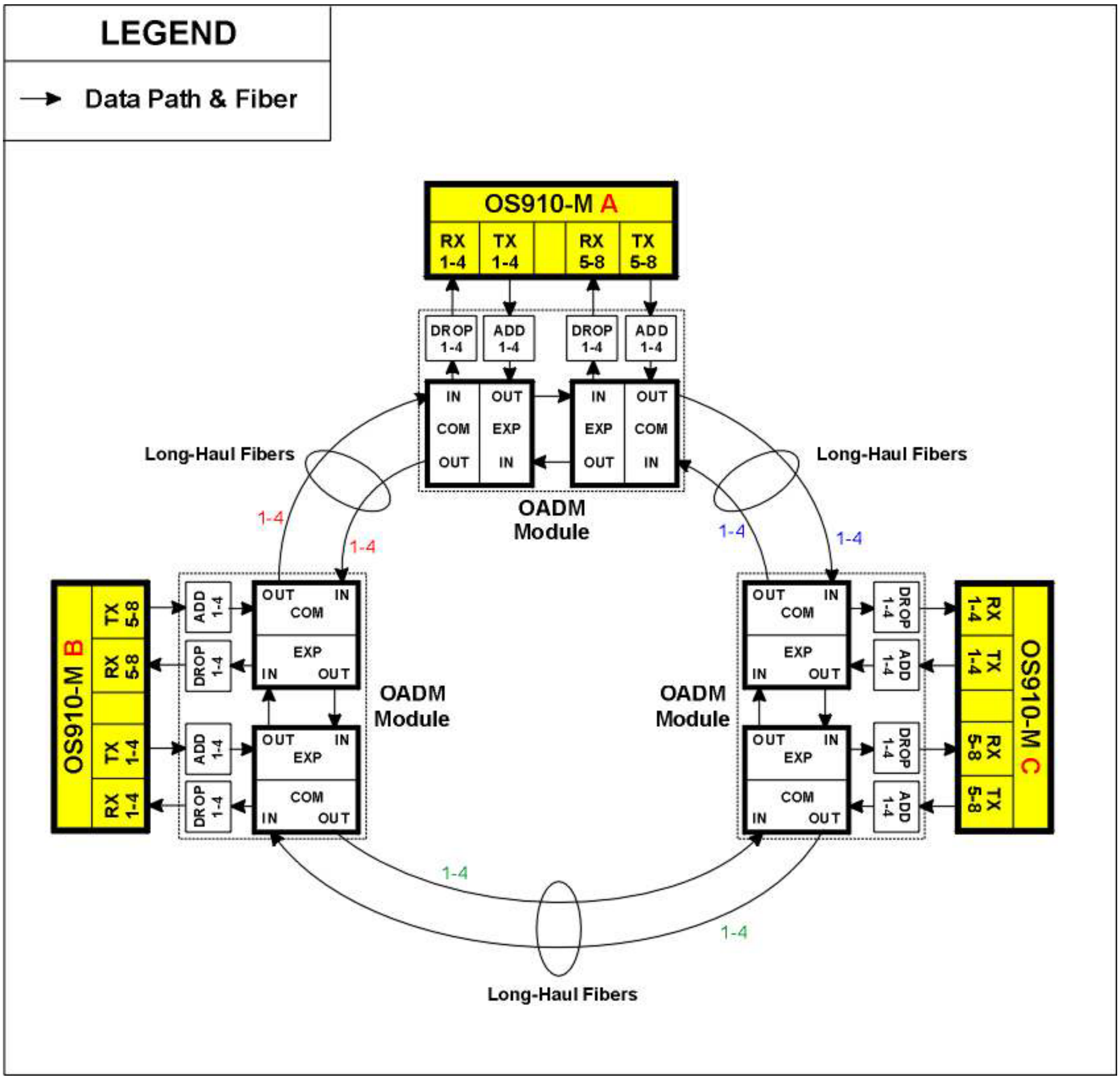



**Figure 58: Data Flow in a WDM Ring Topology having Fiber Redundancy**

# Chapter 38: E1/T1 CES Module

## Applicability

The E1/T1 CES module applies to OS910-M only.

## Terminology

**E1:** European digital transmission format of *thirty-two* 8-bit voice channels (time slots) together having a total bandwidth of 2.048 Mbps.

**T1:** American digital Transmission format of *twenty-four* 8-bit voice channels (time slots) together having a total bandwidth of 1.544 Mbps.

**CES:** (**C**ircuit-**E**mulation **S**ervice) Service that emulates *synchronous* circuits (e.g., E1 or T1) over *asynchronous* networks (e.g., Ethernet).

**Pseudowire Network:** An emulated synchronous circuit (e.g., E1 or T1) in a packet-switching network.

**Pseudowire:** Stream of packets (in a pseudowire network) between two E1/T1 CES modules and containing data from one or more synchronous E1/T1 channels.

**Session:** Specification of the source E1/T1 CES module port, pseudowire packet format, maximum jitter, header format, and address of target E1/T1 CES module.

**Gateway:** A device interfacing networks of different protocols and functioning as a protocol converter in order to provide interoperability of systems interconnected across the networks.

**TDM:** (**T**ime-**D**ivision **M**ultiplexing) A method of placing multiple data streams in a single signal. The segments of each specific stream are time-separated from one another by segments of other streams in a periodic manner. At the receiving end, the segments of each data stream are reassembled using timing.

## Overview

### Purpose

The E1/T1 CES module is an E1/T1 CES gateway TDM for IP/Ethernet networks. It is used to perform the following primary functions:

- Multiplex voice/data signals coming from *local* E1/T1 channels and send them over Ethernet
- Receive multiplexed voice/data signals coming from *remote* E1/T1 channels over Ethernet and demultiplex them to their respective local E1/T1 channels.

### Models

The models of the E1/T1 CES Module for the OS910-M are described in *Table 1*, below.

**Table 28: Models of the E1/T1 TDM Module**

| Model | Description |
|---|---|
| EM9-CES-4E1 | *4*-port *E1* Circuit Emulation Service TDM over packet.<br>Can operate up to thirty-two pseudowire sessions. |
| EM9-CES-4E1c | *4*-port *E1* Circuit Emulation Service TDM over packet with high-precision *clock*.<br>Can operate up to thirty-two pseudowire sessions. |
| EM9-CES-4T1 | *4*-port *T1* Circuit Emulation Service TDM over packet.<br>Can operate up to thirty-two pseudowire sessions. |
| EM9-CES-4T1c | *4*-port *T1* Circuit Emulation Service TDM over packet with high-precision *clock*.<br>Can operate up to thirty-two pseudowire sessions. |

# Application

## General

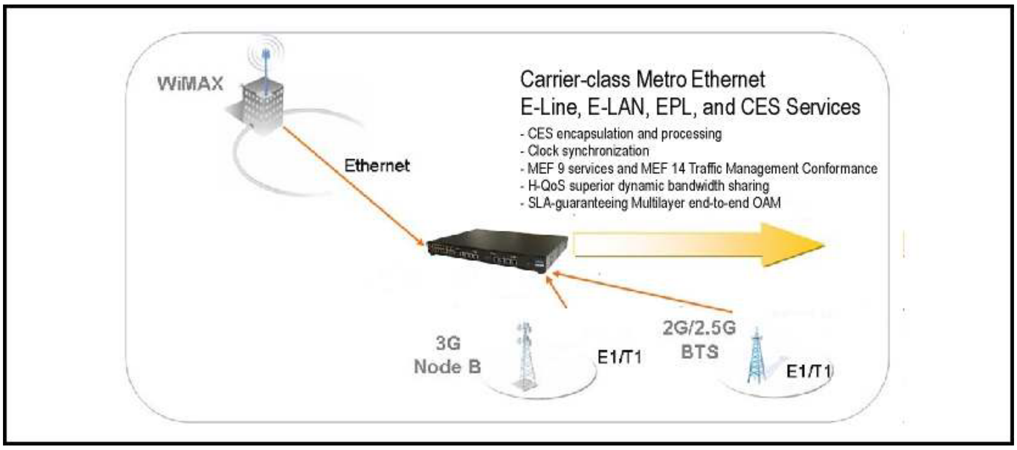



**Figure 59: E1/T1 CES over Ethernet**

## Specific

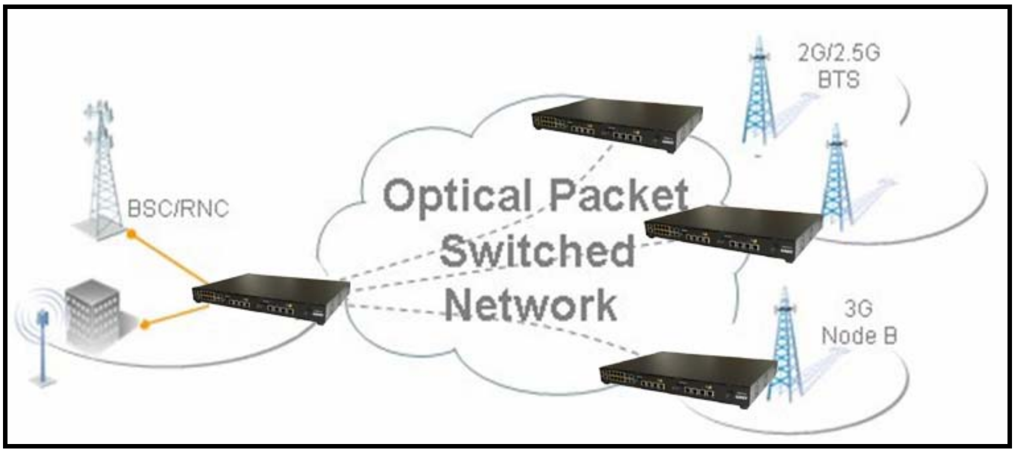



**Figure 60: Cellular Backhaul for GSM, UMTS and GPRS Networks**

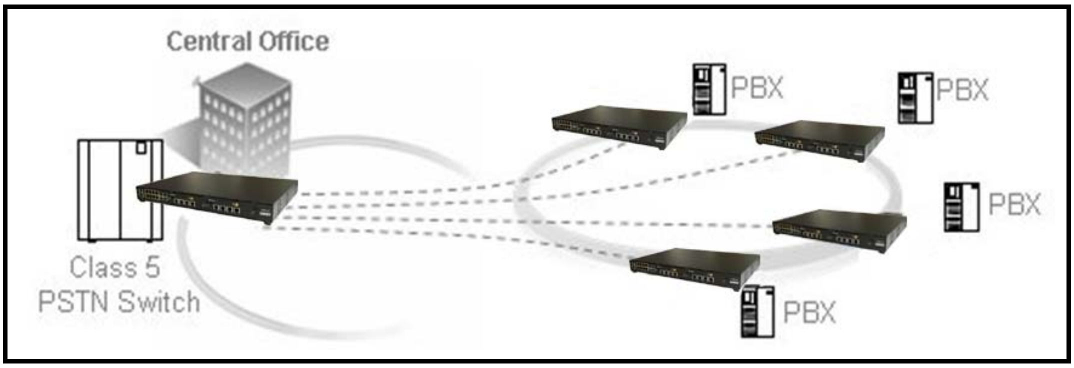



**Figure 61: PSTN-to-PBX and PBX-to-PBX over Ethernet**

# Network Topologies

## Point-to-Point

In the *point-to-point* topology two E1/T1 CES modules are interconnected over an Ethernet network.

## Star

In the *star* topology one E1/T1 CES 4-port module is connected to multiple E1/T1 CES modules over an Ethernet network. The multiple E1/T1 CES modules can be 1-port or 4-port models.

# Requirements

- 6-inch flat-tip screwdriver (for fastening clock input)
- One OS910-M for housing up to two E1/T1 CES modules
- E1/T1 CES modules (per the network topology)
- For external clock input: RG-174 cable with SMB male connector, up to 5 m (16.5 ft), and having 50 Ω impedance (1 cable per E1/T1 CES module)
- Ethernet cables (per the network topology)

# Layout

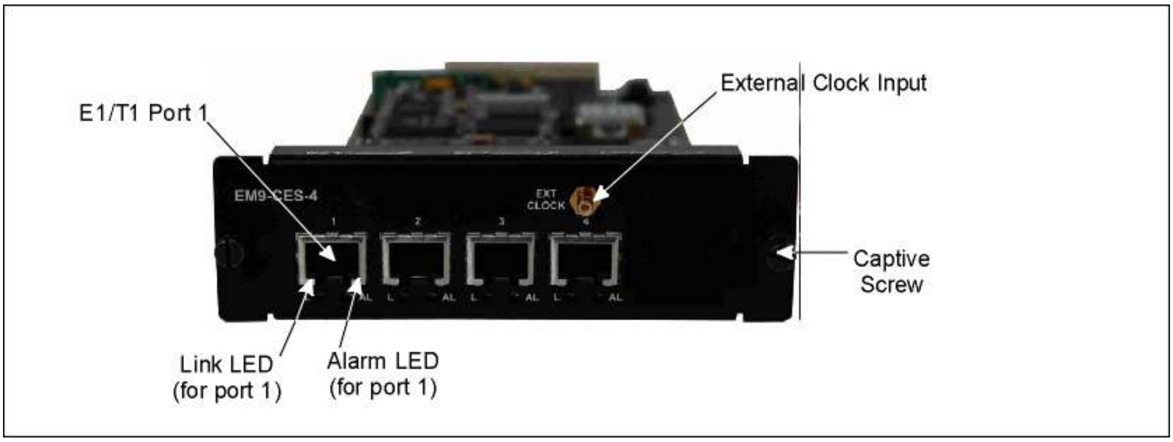



**Figure 62: E1/T1 CES module (EM9-CES-4) Layout**

# Mounting

1. Choose slot 2 or 3[84] in the OS910-M into which the E1/T1 CES module is to be inserted.
2. If a Blank Panel is covering the slot, using a philips screwdriver no. 1 remove it by undoing the *two* philips screws.
3. Holding the E1/T1 CES module with the right side up, place the edges of the module's PCB between the left and right rails in the slot and slide it until its panel is level with the front panel of the OS910-M. (This assures that the module's connector is inserted into place.)
4. In instances that the OS910-M is powered on when the E1/T1 CES module is inserted, invoke the following command:

   **`tdm module insert slot SLOT`**

   where,

   **`SLOT`**: ID (number) of slot into which the E1/T1 CES module has just been inserted. The ID can be **`2`** or **`3`**.
5. With a flat-head No.1 screwdriver, fasten the E1/T1 CES module with the two captive screws located on its edges.

# Dismounting

1. In instances that the OS910-M is powered on when the E1/T1 CES module is to be dismounted, invoke the following command:

   **`tdm module remove slot SLOT`**

   where,

   **`SLOT`**: ID (number) of slot from which the E1/T1 CES module is to be removed. The ID can be **`2`** or **`3`**.
2. With a flat-head No.1 screwdriver, release the E1/T1 CES module by unfastening the two captive screws located on its edges.
3. Holding the E1/T1 CES module by the two screw standoffs, pull it out.

# Cabling

1. Connect the E1/T1 lines from the PSTNs/PBXs to the E1/T1 ports of the E1/T1 CES modules with the wood-pulp or plastic insulation twisted wire-pair cables having RJ48 or RJ45 8-pin male connectors. Make sure that an Ethernet port in each OptiSwitch is connected to the IP/Ethernet network across which the E1/T1 traffic is to be sent.
2. Optionally, connect an external clock source input (shown in *Figure 62*, page *631*).
3. Connect the Ethernet ports of the OS910-Ms to Ethernet network.

# Power

Make sure that the OS910-Ms are powered up.

[84] Slots 2 and 3 are indicated in the *Front* view of the OS910-M, page *63*.

# LEDs

**Table 29: Front Panel LEDs**

| LEDs | | Significance |
|---|---|---|
| **L** (Link) | **AL** (Alarm) | |
| ON-Green | OFF | Link to TDM port OK. |
| ON-Green | ON-Red | *Red alarm* due to framing error.<br>(*Red alarm* means that the EM9-CES is unable to recover the framing reliably. As a result, connectivity to the EM9-CES is lost. *Red alarm* is caused by corruption or loss of signal. In this state, the status of connectivity to the far end is not known.) |
| OFF | ON-Red | *Red alarm* due to loss of carrier. |
| OFF | ON-Yellow | *Yellow alarm*.<br>(*Yellow alarm* means that a *Red alarm* is present at the far end of the link. There is reception from the far end of a data or framing pattern that reports the far end is in the *Red alarm* state. *Red alarm* and *Yellow alarm* states cannot coexist on the same EM9-CES because the *Yellow alarm* pattern must be received within a framed signal.) |
| ON-Green | BLINKING-Yellow | *Blue alarm*.<br>(*Blue alarm* means that the incoming signal is absent. There is a disruption in the communication path between the terminal equipment connected to the EM9-CES. Communication integrity is maintained but no framing to the terminal equipment is provided. |
| BLINKING-Green | Yellow | Port in loopback mode. |

# Principle of Operation

## Pseudowire Modes

There are two modes in which a pseudowire can be formed:

- Unstructured
- Structured

### Unstructured

In unstructured mode all channels (timeslots) from a port are assigned to one destination. The bit stream is packetized according to the session header and other session parameters and then sent to the Packet-Switching Network (PSN). The packet stream has no discernible channel boundaries or any other signaling information.

### Structured

In structured mode, all channels or specific channels from a port can be sent to the destination. The E1/T1 CES module at the receiving end of the pseudowire samples the bit stream on the basis of the type of PCM (whether for E1 or T1) specified in the session . The E1/T1 CES module uses this basis to obtain the signaling information, strips the bit stream of its signaling information, and sends only the data. When necessary it sends a signaling packet stream to indicate change in signaling information.

## TDM over Packet Session

The source and target TDM modules require matching session specifications. According to these specifications, the TDM-over-Packet application divides the E1 or T1 data stream received on the

E1/T1 port into pseudowire packets, adds a special header, and transmits the packets via the Ethernet towards the target E1/T1 CES module. The application at the other end of the pseudowire receives the psedowire packets, removes the header, unpacks the data, and transmits it to the E1 or T1 circuit via the E1/T1 ports.

### Packet Header Formats

Packet headers can have any of the following three formats:

- SAToP
- CESoPSN
- CESoETH

#### SAToP

This header format complies with the *IETF PWE3 SAToP* standard for *unstructured* TDM over PSNs. The header requires 62 bytes per packet, including Ethernet, IP, UDP, and RTP headers and the *SAToP* control word.

#### CESoPSN

This header format complies with the *IETF PWE3 CESoPSN* standard for *structured* TDM over PSNs. The header requires 62 bytes per packet, including Ethernet, IP, UDP, and RTP headers and the *CESoPSN* control word.

#### CESoETH

This header format complies with the *MEF 8* specification *Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks*. It supports both *unstructured* and *structured* pseudowires. The header consists of an Ethernet header, an emulation circuit definition (ECID), and a CESoETH control word having a length of 22 bytes.

## Interfaces

### Names

Two VLAN interfaces are reserved for two E1/T1 CES modules in an OS910-M. These VLAN interfaces are TDMS**2L** and TDMS**3L**. Their relation to configuration, management, and the slots in the OS910-M housing the E1/T1 CES module are shown in *Table 30*, below.

**Table 30: OS910-M-controlled VLAN Interfaces for E1/T1 CES modules**

| | **Slot 2** | **Slot 3** |
|---|---|---|
| **CES Management** | TDMS**2L** | TDMS**3L** |

If no E1/T1 CES module is inserted (sensed) in slot **2** the VLAN interface TDMS**2L** is not created. The VLAN interface is created automatically when an E1/T1 CES module is inserted in slot **2**.

Similarly, if no E1/T1 CES module is inserted (sensed) in slot **3** the VLAN interface TDMS**3L** is not created. The VLAN interface is created automatically when an E1/T1 CES module is inserted in slot **3**.

*The user cannot manipulate these VLAN interfaces in any other way!*

To view these interfaces:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show interface`**

Example

```
OS910-M# show interface

INTERFACES TABLE
```

```
================

Name     M Device       IP                State MAC               Tag  Ports
-------------------------------------------------------------------------------
TDMS2L.    vif4092      10.10.10.33/28      UP   00:0F:BD:FF:53:B7 4092
TDMS3L.    vif4093      10.10.10.49/28      UP   00:0F:BD:FF:53:B7 4093
vif0       vif0         -                   UP   00:0F:BD:00:53:B7 0001 1,3-4

- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

OS910-M#
```

The two VLAN interfaces `TDMS2L` and `TDMS3L` are displayed as in the above example when two E1/T1 CES modules are present in the OS910-M.

### Tags

When E1/T1 CES modules are inserted into an OS910-M, VLAN tags are automatically assigned to the VLAN interfaces of the E1/T1 CES modules according to *Table 31*, below. The user cannot assign these VLAN tags to other VLAN interfaces while the E1/T1 CES modules are in the slots.

**Table 31: VLAN Names and Associated VLAN Tags**

| VLAN Names | VLAN Tags |
|---|---|
| TDMS**2L** | 409**2** |
| TDMS**3L** | 409**3** |

### Interface Subnet

The interface subnet 10.10.10.0/24 is reserved for the VLAN interfaces TDMS**2L** and TDMS**3L**. During initialization[85] of the E1/T1 CES modules, the VLAN interfaces TDMS**2L** and TDMS**3L** are set to be in the UP state permanently. This is the final state of the VLAN interfaces required for the E1/T1 CES modules to operate properly.

## Configuration

### E1 or T1 Mode Selection

To select E1 or T1 mode for the E1/T1 CES module:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`tdm mode (e1|t1) slot (2|3)`**

   where,

   **`(2|3)`**: Number of the slot occupied by the E1/T1 CES module. Valid numbers are 2 and 3.

| | **Note** |
|---|---|
| | Execution of this command will erase the TDM configuration of the E1/T1 CES module. |

85 Initialization of the E1/T1 CES modules starts when the hosting OS910-M is powered up.

Example

```
OS910-M# tdm mode e1 slot 2
TDM configuration will be lost.
Do you want to proceed? (y|n)
y
The operation takes about 50 sec.
To complete this operation the configuration should be saved
and the device should be rebooted.
Would you like to save configuration and reboot the system now? (y|n)
y
Building Configuration...
[OK]

Wait please, system is going to reboot...

Wait please, system is going to reboot
OS910-M#
```

## TDM Mode Entry

To configure a E1/T1 CES module, first enter the TDM mode from **`configure terminal`** mode by invoking the following command:

**`tdm SLOT-NUM`**

where,

**`SLOT-NUM`**: Number of the slot occupied by the E1/T1 CES module. Valid numbers are 2 and 3.

Example

```
OS910-M# configure terminal
OS910-M(config)# tdm 2
OS910-M(config-tdm2)#
```

## Clock Mode Setting

### Single-Clock Domain

Ina *single*-clock domain, select the clock mode for the bit streams by invoking the command:

**`clock mode (external|internal|line1| recovery)`**

where,

**`external`**: use clock provided by the administrator or the E1/T1 CES module in the other slot of the OS910-M.

**`internal`**: use the E1/T1 CES module’s internal clock as a source.

**`line1`**: use the clock received on port 1 as the transmit clock for all ports.

**`loopback`**: use the local E1/T1 CES Module LIU clock received on the E1/T1 port.

**`recovery`**: use the recovered clock produced by the adaptive clock recovery algorithm as the Tx (transmit) clock. This command argument sets the E1/T1 CES Module in Slave mode.

Example

```
OS910-M(config-tdm2)# clock mode line1
OS910-M(config-tdm2)#
```

### Multiple-Clock Domain

In a *multiple*-clock domain, select the clock mode for the bit streams by invoking the command:

**`clock mode (loopback|recovery) PORT`**

where,

**`loopback`**: use the local E1/T1 CES Module LIU clock received on the E1/T1 port.

**recovery**: use the recovered clock produced by the adaptive clock recovery algorithm as the Tx (transmit) clock. This command argument sets the E1/T1 CES Module in Slave mode.

**PORT**: assign the clock mode to a specific TDM port of the E1/T1 CES Module.

Example

```
OS910-M(config-tdm2)# clock mode recovery
OS910-M(config-tdm2)#
```

## IP Address Assignment to a E1/T1 CES Module

An IP address must be assigned to the E1/T1 CES Module following clock settings. The IP address is required for operating in the CES protocols at Layer 2 and Layer 3.

To assign an IP address to the E1/T1 CES Module, assign an IP address to a VLAN interface by invoking the command:

**module-ip A.B.C.D/M interface vifN**

where,

**A.B.C.D/M**: E1/T1 CES module IP address with subnet prefix. This IP address should belong to a subnet configured on one of the OS910-M VLAN interfaces.

**vifN**: ID of existing VLAN interface having the format **vifX**, where **X** is a decimal number in the range **1-4089**. Example: **vif3**. The IP address of the interface must belong to the same subnet on which the E1/T1 CES module resides. This VLAN interface will be permanently in the UP state.

Example

```
interface vlan vif10
 tag 10
 ip 1.1.1.1/8
 port 1

tdm 2
 clock mode internal
 module-ip 1.1.1.10/8 interface vif10
 session s1 description port_1
 session s1 port 1
 session s1 header-proto l3 target-ip 2.2.2.10
 session s1 local-udp-port 49152
 session s1 target-udp-port 49152
```

In the above example, an E1/T1 CES module is in slot 2 (as indicated by the `2` in `tdm 2`). The IP address assigned to the E1/T1 CES module is `1.1.1.10`, taken from the interface subnet of the VLAN interface `vif10`.

`vif10` will remain permanently UP independently of its member port 1, i.e., even if the port has no link, is unconnected, or connected to another device! Accordingly, `vif10` can be configured without any port as a member as shown for VLAN interfaces `vif6` and `vif8` in the section *Configuration Example 3,* page *662*.

## Deleting IP Address Assigned to a E1/T1 CES Module

To delete the IP address assigned to the E1/T1 CES Module, invoke the command:

**no module-ip**

Example

```
OS910-M(config)# tdm 2
OS910-M(config-tdm2)# no module-ip
OS910-M(config-tdm2)#
```

## External Clock Input Selection

If an external clock is to be used, specify the clock source by invoking the command:

**clock input-ext (default|bnc|other-slot-recovered)**

where,

**`default`**: Ignore external clock. Default.

**`bnc`**: Select the external clock source connected to the E1/T1 CES Module.

**`other-slot-recovered`**: Select the clock from neighbor slot (set using the command **`clock output bnc`** or **`clock mode recovery`**).

Example

```
OS910-M(config-tdm2)# clock input-ext other-slot-recovered
OS910-M(config-tdm2)#
```

## Clock Exportation

When **`clock mode`** is set to **`external`**, **`recovery`**, or **`line1`** source mode, the received clock can be exported to the E1/T1 CES module located in the neighbor slot by invoking the command:

**`clock output (default|bnc|recovered)`**

where,

**`default`**: Do not export the clock to the neighbor slot. Default.

**`bnc`**: Export the clock from the external clock source to the neighbor slot.

**`recovered`**: Export *recovered* clock (set using the command **`clock mode recovery`**) or *TDM* clock (set using the command **`clock mode line1`**) for the neighbor slot.

Example

```
OS910-M(config-tdm2)# clock output recovered
OS910-M(config-tdm2)#
```

## Transport Emulation Type Configuration

Transport emulation can be configured either in unstructured or structured mode. In unstructured mode, the entire E1/T1 circuit is transferred regardless of frame structure and time slot boundaries. This is called “structure agnostic” emulation. In structured mode, full or fractional frames can be packetized and transferred to the E1/T1 CES Modules.

E1 and T1 data is structured as frames based on 8 KHz frame synchronization (sampling rate). Each frame is divided into 8-bit time slots (32 slots for E1, 24 slots for T1). The traffic is depacketized at the other end of the pseudowire to reconstruct frames with the selected time slots in their corresponding time slot positions.

To select the pseudowire mode, invoke the command:

**`port PORT transport-emulation-type (struct|unstruct|default)`**

where,

**`PORT`**: Number of E1 or T1 port in the E1/T1 CES Module.

**`struct`**: Structured (framed) pseudowire mode.

**`unstruct`**: Unstructured (unframed) pseudowire mode.

**`default`**: Pseudowire mode set by E1/T1 CES Module. (Default.)

Example

```
OS910-M(config-tdm2)# port 4 transport-emulation-type struct
OS910-M(config-tdm2)#
```

## Port LIU Channel Bandwidth Configuration

A T1 frame consists of 193 bits: 8 x 24 time slots plus the F-bit. The F-bit is not sent in a pseudowire. When the E1/T1 CES Module operates in T1 and the channel bandwidth is 64 Kbps, all eight bits of a time slot are dedicated to data. If the channel bandwidth is configured for 56 Kbps, the F-bit is used for channel associated signaling and transmitted out-of-stream. This configuration is valid for T1 ports in structured mode only!

To select the channel bandwidth, invoke the command:

**`port PORT liu-channel-bandwidth (64K|56K|default)`**

where,

**`PORT`**: Number of T1 port in the E1/T1 CES Module.

**64K**: Framed 64 Kbps for T1 only.
**56K**: Framed 56 Kbps for T1 only.
**default**: Channel bandwidth set by E1/T1 CES Module. (Default.)

Example

```
OS910-M(config-tdm2)# port 4 liu-channel-bandwidth 64K
OS910-M(config-tdm2)#
```

## Port LIU Frame Format Setting

For each E1 port, the framing format PCM30 or PCM31can be selected.

For each T1 port, the framing format D4 or ESF can be selected.

T1 Framing

The Extended Super Frame (ESF) mode and the D4 mode are valid for T1 in the structured mode. The T1 data is divided into 24 time slots, each of 8 bits, thus totaling 192 bits. The selected protocol defines a bit pattern in the 193rd bit across a predetermined number of frames. When the port has a channel data rate of 64 Kbps, all eight bits of the channel are dedicated; no signaling information is carried. However, when the port has a channel rate of 56 Kbps, only seven bits of the channel are dedicated, and the eighth bit is reserved for signaling information, contained in the "not sent bit t" in every sixth frame.

E1 Framing

The E1 data, in PCM 30 format, divided into 32 time slots, each of 8 bits. Each of the time slot sends and receives an 8-bit sample 8000 times per second. One timeslot (TS0) is reserved for framing purposes, and alternately transmits a fixed pattern. This allows the receiver to lock onto the start of each frame and match up each channel in turn. The standard allows for a full Cyclic Redundancy Check to be performed across all bits transmitted in each frame, and to detect whether the circuit is losing bits (information). Another timeslot (TS16) is reserved for signaling purposes, to control call setup and tear down according to one of several standard telecommunications protocols.

To set the frame format, invoke the command:

**port PORT liu-frame-format (e1_pcm30|e1_pcm31|t1_d4|t1_esf|default)**

where,

**PORT**: Number of E1 or T1 port in the E1/T1 CES Module .
**e1_pcm30**: Framing format PCM30 (for E1 only).
**e1_pcm31**: Framing format PCM31 (for E1 only).
**t1_d4**: Framing format D4 (for T1 only).
**t1_esf**: Framing format ESF (for T1 only).
**default**: Frame format set by E1/T1 CES Module. (Default.)

Example

```
OS910-M(config-tdm2)# port 4 liu-frame-format e1_pcm30
OS910-M(config-tdm2)#
```

## Port LIU Receive Equalizer Gain Limit

The LIU Receive Equalizer Gain Limit to be set for a port depends on the characteristics of the line connected to the port.

To set the LIU Receive Equalizer Gain Limit, invoke the command:

**port PORT liu-gain-limit (short|long|default)**

where,

**PORT**: Number of E1 or T1 port in the E1/T1 CES Module.
**long**: For E1: -43dB; For T1: -36dB
**short**: For E1: -15dB; For T1: -15dB
**default**: LIU Receive Equalizer Gain Limit set by E1/T1 CES Module. (Default.)

Example

```
OS910-M(config-tdm2)# port 4 liu-gain-limit long
OS910-M(config-tdm2)#
```

## Port LIU Line Build Out Configuration

LIU Line Build Out function for a port depends on the impedance or length of the E1 or T1 line between the E1/T1 CES Module and the E1/T1 source.

E1 options: E1_75, E1_120, E1_75_HRL, or E1_120_HRL.

T1 options: T1_133, T1_266, T1_399, T1_533, T1_655, T1_7.5, T1_15, or T1_22.5.

For a T1 port, the cable must be coax with 75Ω impedance. The T1 port must be fitted with an external balloon. For the remaining options impedances are software configurable.

To set the LIU Line Build Out function for an *E1* line, invoke the command:

**port PORT liu-line-build-out (e1_75|e1_120|e1_75_hrl|e1_120_hrl)**

where,

**PORT**: Number of E1 port in the E1/T1 CES Module.

To set the LIU Line Build Out function for an *T1* line, invoke the command:

**port PORT liu-line-build-out (t1_133|t1_266|t1_399|t1_533|t1_655|t1_7.5|t1_15|t1_22.5)**

where,

**PORT**: Number of T1 port in the E1/T1 CES Module.

To set the LIU Line Build Out function for an E1 or T1 line to the *default value*, invoke the command:

**port PORT liu-line-build-out default**

## Port LIU Line Code Configuration

This configures LIU line coding for the E1/T1 ports

**port PORT liu-line-coding (hdb3|ami|b8zs|default)**

where,

**PORT**: Number of E1 or T1 port in the E1/T1 CES Module.

**ami**: AMI for E1 and T1.

**b8zs**: B8ZS for T1 only.

**hdb3**: HDB3 for E1 only.

**default**: Line Code set by E1/T1 CES Module. (Default.)

## Enabling an E1/T1 Port

By default, an E1/T1 port is enabled. To enable an E1/T1 port, invoke the command:

**port PORT state enable**

where,

**PORT**: Number of E1 or T1 port in the E1/T1 CES Module.

## Disabling an E1/T1 Port

To disable an E1/T1 port, invoke the command:

**port PORT state disable**

where,

**PORT**: Number of E1 or T1 port in the E1/T1 CES Module.

## Loopback Mode for an E1/T1 Port

To set an E1/T1 port in loopback mode, invoke the command:

**port PORT loopback (diagnostic|disable|line)**

where,

**disable**: Loopback disable (default).

**`diagnostic`**: Diagnostic (local) mode, i.e., enable local loopback at port.

**`line`**: Line (remote) mode, i.e., enable remote loopback from port.

## Creating a New Session

To create a new pseudowire session, invoke the command:

**`session NAME description DESCR`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`DESCR`**: Alphanumeric string of up to 31 characters.

To enable a session a port must be assigned to it!

## Deleting a Session

To delete an existing session, invoke the command:

**`no session NAME`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

Example

```
OS910-M(config-tdm2)# no session s05
OS910-M(config-tdm2)#
```

## E1/T1 Port Assignment to a Session

Session activation on a specific E1/T1 port depends on whether the port is configured to structured or unstructured mode.

In unstructured mode all timeslots from the port are assigned to one destination. The data stream from the port, by definition, has no discernible time slots or other signaling information. The data stream is packetized according to the session header and other session parameters and then sent to the PSN.

In structured mode, all or a portion of the traffic from the port can be sent to the target destination.

To assign an E1/T1 port to a session in *structured mode with all timeslots* or in *unstructured* mode, invoke the command:

**`session NAME port PORT`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`PORT`**: E1/T1 port number in the module.

To assign an E1/T1 port to a session in *structured mode with some timeslots*, invoke the command:

**`session NAME port PORT timeslots VALUE`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`PORT`**: E1/T1 port number on the TDM module.

**`VALUE`**: Timeslots list.

Example

```
OS910-M(config-tdm2)# session s05 port 4
OS910-M(config-tdm2)#

OS910-M(config-tdm2)# session s06 port 3 timeslots 2-10
OS910-M(config-tdm2)#
```

The session is enabled once a port is assigned to it!

## Setting CES Protocol Header Format and Target Address

To set a SAToP or CESoPSN Header Format and a Target Address, invoke the command:

**`session NAME header-proto l3 target-ip A.B.C.D`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`l3`**: CES using Layer 3 SAToP or CESoPSN session header format.

**`A.B.C.D`**: Target IP address.

To set a CESoETH Header Format and a Target Address, invoke the command:

**`session NAME header-proto l2 target-mac MAC_ADDRESS`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`L2`**: CES using Layer 2 CESoETH session header format.

**`MAC_ADDRESS`**: Target MAC address in the format xx:xx:xx:xx:xx:xx, where x is a hexadecimal digit, e.g., 8b: d0:e3:ac:28:f9.

Example

```
OS910-M(config-tdm2)# session s03 header-proto l2 target-mac 00:12:72:00:5e:4e
OS910-M(config-tdm2)#

        or

OS910-M(config-tdm2)# session s02 header-proto l3 target-ip 60.1.1.2
OS910-M(config-tdm2)#
```

## Modifying the Description of an Existing Session

To modify the description of an existing session, invoke the command:

**`session NAME description DESCR`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`DESCR`**: Description. String upto 31 characters.

Example

```
OS910-M(config-tdm2)# session s05 description TEST-SESSiON-2
OS910-M(config-tdm2)#
```

## Setting a Session's UDP Local Port

To set a session's UDP *local* port, invoke the command:

**`session NAME`** ***`local`*** **`-udp-port (UDP-PORT)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`UDP-PORT`**: UDP local port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm2)# session s02 local-udp-port 49152
OS910-M(config-tdm2)#
```

## Setting a Session's UDP Target Port

To set a session's UDP *target* port, invoke the command:

**`session NAME`** ***`target`*** **`-udp-port (UDP-PORT)`**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**UDP-PORT**: UDP target port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm2)# session s02 target-udp-port 49152
OS910-M(config-tdm2)#
```

## Setting a Session's Out-of-stream (Signaling) UDP Local Port

To set a session's out-of-stream (signaling) UDP local port, invoke the command:

**session NAME local-oos-udp-port (UDP-PORT)**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**UDP-PORT**: UDP target port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm2)# session s02 local-oos-udp-port 49152
OS910-M(config-tdm2)#
```

## Setting a Session's Out-of-stream (Signaling) UDP Target Port

To set a session's out-of-stream (signaling) UDP target port, invoke the command:

**session NAME target-oos-udp-port (UDP-PORT)**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**UDP-PORT**: UDP target port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm2)# session s02 target-oos-udp-port 49152
OS910-M(config-tdm2)#
```

## Setting the IP-ToS Field in the IP header of the CES Packet

The IP ToS field controls the priority of the CES traffic in an L3 session.

To set the IP ToS field, invoke the command:

**session NAME ip-tos (TOS)**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**TOS**: IP ToS value selectable from the range 0 to 255.

Example

```
OS910-M(config-tdm2)# session s02 ip-tos 184
OS910-M(config-tdm2)#
```

## Setting the *Local* Emulation Circuit ID for Unstructured Mode

To set the *local* Emulation Circuit ID (ECID) for a CESoETH Header in *unstructured* mode[86], invoke the command:

**session NAME local-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

[86] Data and signaling are sent in the same session.

Example

```
OS910-M(config-tdm2)# session s2 local-ecid 20
OS910-M(config-tdm2)#
```

## Setting the *Remote* Emulation Circuit ID for Unstructured Mode

To set the *remote* Emulation Circuit ID (ECID) for a CESoETH Header in *unstructured* mode, invoke the command:

**session NAME target-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm2)# session s2 target-ecid 20
OS910-M(config-tdm2)#
```

## Setting the *Local* Emulation Circuit ID for Structured Mode

To set the *local* Emulation Circuit ID (ECID) for a CESoETH Header in *structured* mode[87], invoke the command:

**session NAME local-oos-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm2)# session s2 local-oos-ecid 25
OS910-M(config-tdm2)#
```

## Setting the *Remote* Emulation Circuit ID for Structured Mode

To set the *remote* Emulation Circuit ID (ECID) for a CESoETH Header in *structured* mode, invoke the command:

**session NAME target-oos-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm2)# session s2 target-oos-ecid 25
OS910-M(config-tdm2)#
```

## Setting the Maximum Jitter Delay for a Session

To set the maximum jitter in milliseconds allowed for a session, invoke the command:

**session NAME jitter (MSEC)**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**MSEC**: Max jitter delay selectable from the range 1 to 64).

[87] For E1, in PCM-30 mode, data and signaling are sent in separate sessions.

Example

```
OS910-M(config-tdm2)# session s02 jitter 10
OS910-M(config-tdm2)#
```

## Setting the Number of TDM Frames in Payload

To set the maximum number of E1/T1 frames in the payload for a session, invoke the command:

**`session NAME payload-length (NUM)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`NUM`**: Number of TDM frames in payload.

For E1 the maximum allowed is 25.

For T1 the maximum allowed 33.

Example

```
OS910-M(config-tdm2)# session s02 payload-length 16
OS910-M(config-tdm2)#
```

## Enabling/Disabling Payload Suppression

To enable or disable payload-suppression for a session, invoke the command:

**`session NAME payload-suppression (enable|disable|default)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`enable`**: Enable payload suppression.

**`disable`**: Disable payload suppression.

**`default`**: Disable payload suppression.

Example

```
OS910-M(config-tdm2)# session s02 payload-suppression enable
OS910-M(config-tdm2)#
```

## Enabling/Disabling RTP Header Enable/Disable

To enable or disable RTP Header, invoke the command:

**`session NAME rtp-header (enable|disable|default)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`enable`**: Enable RTP header.

**`disable`**: Disable RTP header.

**`default`**: Disable RTP header.

Example

```
OS910-M(config-tdm2)# session s02 rtp-header enable
OS910-M(config-tdm2)#
```

## Enabling or Disabling a Session

To enable or disable a session, invoke the command:

**`session NAME state (enable|disable)`**

where,

**`PORT`**: E1/T1 port number in the module.

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`enable`**: Enable state.

**`disable`**: Disable state.
**`default`**: Disable state.

Example

```
OS910-M(config-tdm2)# session s02 state enable
OS910-M(config-tdm2)#
```

## VLAN Tag and Priority for a Session

To assign a VLAN ID and VLAN Priority Tag to a session, invoke the command:

**`session NAME vlan VLAN-ID vpt VPT`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`VLAN-ID`**: VLAN ID/tag (in the range **`1`** to **`4091`**). The packets of the session are transmitted to the Ethernet network with this ID.

**`VPT`**: VLAN Priority Tag (in the range **`0`** to **`7`**). The packets of the session are transmitted to the Ethernet network with this priority.

Example

```
OS910-M(config-tdm2)# session s3 vlan 10 vpt 4
OS910-M(config-tdm2)#
```

## Recovery Clock

General

The clock rate of a TDM circuit over a pseudowire must be consistent so that there is no overflow or underflow due to clock differences. That is, the clock rate for the TDM data transmitted at one end of the emulated circuit (Tx clock) must be the same as the clock rate of the same TDM stream received at the other end of the emulated circuit (Rx clock).

To maintain clock continuity of the E1/T1 circuits across a PSN and to meet the ITU G.823 and G.824 standards, the E1/T1 CES Module recovers the clock from the pseudowire data stream. One E1/T1 CES Module is designated as Master while the others are designated as Slaves. Slave E1/T1 CES Modules derive the local Tx clock from the received pseudowire packets.

The E1/T1 CES Module employs an adaptive clock recovery algorithm based on criteria such as: the number of packets received over certain time intervals, the measured Packet Delay Variation (PDV), and the state of the jitter buffer. The algorithm accuracy depends on the 1 Part Per Million (PPM) system clock provided by the module's temperature-compensated crystal oscillator (TCXO). The TCXO is sufficiently accurate to meet the ITU standards for jitter and wander. If a more stringent standard is to be met, a more accurate and stable clock source, such as the oven-controlled crystal oscillator OCXO, may be provided to the user.

To determine whether the crystal oscillator in the E1/T1 CES Module is of type TCXO or OCXO, in the TDM mode (entered using the command **`tdm SLOT-NUM`**), invoke the command **`show module`**.

Modes

The E1/T1 CES Module can be set to attempt clock recovery in either of the following modes:

| | |
|---|---|
| *Single-Recovery-Clock Mode:* | The single-recovery-clock mode allows the use of one clock (recovered from one currently active session) *for all E1/T1 ports* of a E1/T1 CES Module.<br>A recovery clock has two clock input controllers. The single-recovery-clock mode allows connection of one session (PW-1) to the clock input controller 1 (primary) and a second session (PW-2) to clock input controller 2 (secondary). One clock input controller is active (for example, the controller connected to the session PW-1), while the second serves as backup. The second session will become active instead of the first in the event that the first fails). |
| *Multiple-Recovery-Clocks Mode:* | The multiple-recovery-clocks mode allows the use of one clock (recovered from one currently active session) *per E1/T1 port* of |

a E1/T1 CES Module. The recovery clocks are independent of one another.
Every clock utilizes the primary pseudowire for clock recovery and switches to the secondary pseudowire, if the primary one is disabled by the user.

**Setting Recovery-clock Mode**

To set the mode in which clock recovery will be attempted, invoke the command:

**`recovery-clock independent-domain-cfg (single|multiple)`**

where,

**`single`**: Single-Recovery-Clock Mode.

**`multiple`**: Multiple-Recovery-Clocks Mode.

Example

```
OS910-M(config-tdm2)# recovery-clock independent-domain-cfg single
OS910-M(config-tdm2)#
```

**Connecting a Recovery-clock Controller to a Session**

To connect a recovery-clock controller to a session, invoke the command:

**`recovery-clock session NAME controller (1|2)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`1`**: Connect Controller 1 of the clock (connected to the port) to the session.

**`2`**: Connect Controller 2 of the clock (connected to the port) to the session.

Example

```
OS910-M(config-tdm2)# recovery-clock session s02 controller 1
OS910-M(config-tdm2)#
```

**Disconnecting a Recovery-clock Controller from a Session**

To disconnect a recovery-clock controller from a session, invoke the command:

**`no recovery-clock session NAME controller (1|2)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`1`**: Use controller #1 of the Clock connected to the port attached to session.

**`2`**: Use the controller #2 of the Clock that is connected to the port is attached to session.

Example

```
OS910-M(config-tdm2)# no recovery-clock session s02 controller 1
OS910-M(config-tdm2)#
```

## Default SL

To set the DiffServ level (SL) for CES traffic sent to an Ethernet port to the default value (1, lowest priority), invoke the command:

**`no ces-traffic egress sl`**

Example

```
OS910-M(config-tdm2)# no ces-traffic egress sl
OS910-M(config-tdm2)#
```

## User-defined SL

To set the SL for CES traffic sent to an Ethernet port, invoke the command:

**`ces-traffic egress sl <1-8>`**

where,

**<1-8>**: SL selectable from the range 1 to 8.

Example

```
OS910-M(config-tdm2)# ces-traffic egress sl 8
OS910-M(config-tdm2)#
```

## Routing

If OS910-Ms with E1/T1 CES modules installed in them are used in a routing network, the subnets containing the IP addresses of the E1/T1 CES modules must be excluded from the routing databases. The procedure for each routing protocol is as follows:

### OSPF

1. Enter **configure terminal** mode.
2. Invoke the commands:

```
access-list protocols deny_ces deny 10.10.10.32/28
access-list protocols deny_ces deny 10.10.10.48/28
access-list protocols deny_ces permit any

router ospf
  redistribute connected
  distribute-list deny_ces out
```

### ISIS

1. Enter **configure terminal** mode.
2. Invoke the commands:

```
ip prefix-list CES seq 5 deny 10.10.10.32/28
ip prefix-list CES seq 10 deny 10.10.10.48/28
ip prefix-list CES seq 15 permit any
route-map CES permit 10
  match ip address prefix-list CES

router isis
  redistribute connected route-map CES
```

### BGP

1. Enter **configure terminal** mode.
2. Invoke either of the following set of the commands:

Set 1

```
ip prefix-list CES seq 5 deny 10.10.10.32/28
ip prefix-list CES seq 10 deny 10.10.10.48/28
ip prefix-list CES seq 15 permit any
!
route-map CES permit 10
  match ip address prefix-list CES

router bgp 100
  redistribute connected
  neighbor x.x.x.x prefix-list CES out
```

Set 2

```
ip prefix-list CES seq 5 deny 10.10.10.32/28
ip prefix-list CES seq 10 deny 10.10.10.48/28
ip prefix-list CES seq 15 permit any
route-map CES permit 10
```

```
  match ip address prefix-list CES

router bgp 100
  redistribute connected route-map CES
```

# Viewing

## General Configuration and Status Information

### Viewing Current Mode (E1 or T1)

To view whether the current mode of the E1/T1 CES module is E1 or T1:

1. Enter **enable** mode.
2. Invoke the command:

   **show tdm mode slot (2|3)**

   where,

   **(2|3)**: Number of the slot occupied by the E1/T1 CES module. Valid numbers are 2 and 3.

Example

```
OS910-M# show tdm mode slot 2
Internal config              :  E1
Eeprom config                :  E1
```

### Viewing MAC Address

To view the MAC address of the E1/T1 CES Module, invoke the command:

**show module mac-addr**

Example

```
OS910-M(config-tdm3)# show  module mac-addr

MAC-addr  : 00:12:72:00:5e:54
OS910-M(config-tdm3)#
```

### Viewing Ethernet Statistics

To view the Ethernet statistics of the E1/T1 CES Module, invoke the command:

**show eth-statistics**

Example

```
OS910-M(config-tdm3)# show eth-statistics

Item                                :  Value
------------------------------------------------------
In octets                           :  1627156548
Out octets                          :  1525313958
Frames received                     :  5770059
Frames transmitted                   :  5777704
In multicast                        :  0
Out multicast                       :  0
In broadcast                        :  3
Out broadcast                       :  6
Single collisions                   :  0
Multicast collisions                :  0
Defered frames                      :  0
Excessive defered frames            :  0
late collisions                     :  0
Excessive collisions                :  0
Mac in pause frames                 :  0
Mac out pause frames                :  0
Ip datagram received                :  0
Align errors                        :  0
Crc errors                          :  0
Frames too long                     :  0
Mac rx error                        :  0
Short frames                        :  0
Mac tx errors                       :  0
Code errors                         :  0
Mac in unknown opcode               :  0
Ip header errors                    :  0
Rx fifo overrun                     :  0
Tx underrun                         :  0
Bundle overflow                     :  0
Range length errors                 :  0
Out of range length errors          :  0
Retransmits timeout                 :  0
No buffer discards                  :  0
Rx discards                         :  0
OS910-M(config-tdm3)#
```

### Viewing System Information

To view the system information of the E1/T1 CES Module, invoke the command:

**show module**

Example

```
OS910-M(config-tdm3)# show module-system-info
SW version                    :  AG1624R01.00.00_D017
DB model template             :  R1624ETEA1001
Board Type                    :  18
Board Revision                :  0
CPLD Revision                 :  2
FPGA ID                       :  12
FPGA version                  :  105
CM PLL Type                   :  0
DB product enum               :  5
DB model enum                 :  9
Detect card                   :  1
Redux_board                   :  1
Application ct                :  18
Current system tick           :  592763
Silicon ID                    :  1
Silicon version               :  0
ROM archit                    :  0
MAC-addr                      :  00:12:72:00:5e:54
Shift register value          :  0
OS910-M(config-tdm3)#
```

## Clock

### Viewing Clock Configuration

To view the current clock configuration, invoke the command:

**show clock**

Example

```
OS910-M(config-tdm2)# show clock

Recovery Clock mode : Single.
                    controller: 1; connected session:      ; active:   No;
                    controller: 2; connected session:      ; active:   No;

Clock number: 1, Controller number: 1
------------------------------------------------
Clock mode                    : Internal
Input state                   : Active
Clock input mode              : Free running
Recovery method               : Direct
Input status                  : Not locked
Priority                      : 0
Clock index                   : 1
OS910-M(config-tdm2)#
```

## Port

### Viewing E1/T1 Port LIU Information

To view the configuration and status information on the ports of the E1/T1 CES Module, invoke the command:

**show tdm-ports**

Example

```
OS910-M(config-tdm2)# show tdm-ports

 Clocking_mode :  LINE_1
 LIU line format  :   E1
                          --------------------Configuration Information--------------------

Modified Running_config     :         Port1    Port2    Port3     Port4
-------------------------- :         -----    ------   -----     -----
Port state                  :         Enabled  Enabled  Enabled   Enabled
LIU framer type             :         DS26524  DS26524  DS26524   DS26524
LIU line code               :         HDB3     HDB3     HDB3      HDB3
LIU line build out          :         120NORM  120NORM  120NORM   120NORM
LIU monitor gain            :         NORMAL   NORMAL   NORMAL    NORMAL
LIU Rx equalizer gain limit:          Short    Short    Short     Short
LIU jitter attenuation      :         Disabled Disabled Disabled  Disabled
LIU loopback                :         Disabled Disabled Disabled  Disabled
Framed mode                 :         Unframed Unframed Unframed  Framed
Frame format                :         -        -        -         PCM31
Channel bandwidth           :         -        -        -         Fram_64K
TDM signaling type          :         -        -        -         CCC
OS910-M(config-tdm2)#

                          --------------------Status Information--------------------

Status         :      Port1       Port2        Port3        Port4
---------------:      -----       -----        -----        -----
Port status    :      ACTIVE      ACTIVE       ACTIVE      ACTIVE
Link           :      UP          DOWN         DOWN        DOWN
LIU loopback   :      DISABLE     DISABLE      DISABLE     DISABLE
NoAlarm        :      no alarm    -            -           -
RcvFarEndLOF   :      -           -            -           -
XmtFarEndLOF   :      -           -            -           -
RcvAIS         :      -           -            -           -
XmtAIS         :      -           ais (tx)     ais (tx)    -
LossOfFrame    :      -           -            -           -
LossOfSignal   :      -           los          los         los
LoopbackState  :      -           -            -           -
T16AIS         :      -           -            -           -
RcvFarEndLOMF  :      -           -            -           -
XmtFarEndLOMF  :      -           -            -           -
Others         :      -           -            -           -
OS910-M(config-tdm2)#
```

### Viewing E1/T1 Port LIU Configuration

To view *only* the LIU configuration for the ports of the E1/T1 CES Module, invoke the command:

**`show tdm-ports config`**

Example

```
OS910-M(config-tdm2)# show tdm-ports config

Clocking_mode    : LINE_1
LIU line format  : E1

Modified Running_config    :   Port1      Port2      Port3    Port4
---------------------------:   -----      -----      -----    -----
Port state                 :  Enabled   Enabled   Enabled   Enabled
LIU framer type            :  DS26524   DS26524   DS26524   DS26524
LIU line code              :  HDB3      HDB3      HDB3       HDB3
LIU line build out         :  120NORM   120NORM   120NORM   120NORM
LIU monitor gain           :  NORMAL    NORMAL    NORMAL    NORMAL
LIU Rx equalizer gain limit :  Short     Short     Short     Short
LIU jitter attenuation     :  Disabled  Disabled  Disabled Disabled
LIU loopback               :  Disabled  Disabled  Disabled  sabled
Framed mode                :  Unframed  Unframed  Unframed  Framed
Frame format               :  -         -         -          PCM31
Channel bandwidth          :  -         -         -      Frame_64K
TDM signaling type         :  -         -         -            CCC
OS910-M(config-tdm2)#
```

### Viewing E1/T1 Port LIU Status

To view *only* the LIU status for the ports of the E1/T1 CES Module, invoke the command:

**`show tdm-ports status`**

Example

```
OS910-M(config-tdm2)# show tdm-ports status

Status          :  Port1         Port2         Port3         Port4
---------------:  -----         -----         -----         -----
Port status     :  ACTIVE        ACTIVE        ACTIVE        ACTIVE
Link            :  UP            DOWN          DOWN          DOWN
LIU loopback    :  DISABLE       DISABLE       DISABLE       DISABLE
NoAlarm         :  no alarm      -             -             -
RcvFarEndLOF    :  -             -             -             -
XmtFarEndLOF    :  -             -             -             -
RcvAIS          :  -             -             -             -
XmtAIS          :  -             ais (tx)      ais (tx)      -
LossOfFrame     :  -             -             -             -
LossOfSignal    :  -             los           los           los
LoopbackState   :  -             -             -             -
T16AIS          :  -             -             -             -
RcvFarEndLOMF   :  -             -             -             -
XmtFarEndLOMF   :  -             -             -             -
Others          :  -             -             -             -
OS910-M(config-tdm2)#
```

### Viewing E1/T1 Port LIU Default Configuration

To view the LIU default configuration for the ports of the E1/T1 CES Module, invoke the command:

**`show tdm-ports default-config`**

Example

```
OS910-M(config-tdm2)# show tdm-ports default-config

Items                         :   Default Values
----------------------------- :   -----
LIU line format               :   E1
LIU type                      :   DS26524
LIU line code                 :   HDB3
LIU line build out            :   120NORM
LIU monitor gain              :   NORMAL
LIU Rx equalizer gain limit   :   Short
LIU jitter attenuation        :   Disabled
LIU loopback                  :   Disabled
Framed mode                   :   Unframed
Frame format                  :   -
Channel bandwidth             :   -
TDM signaling type            :   -
OS910-M(config-tdm2)#
```

## Session

### Viewing Sessions

To view the sessions created on the E1/T1 CES Module, invoke the command:

**show session**

Example

```
OS910-M(config-tdm2)# show session

Name Description   modified_config    running_config
------------------------------------------------------------------
S02  SESSiON-2-1   Session Enabled    Session running
S03  SESSiON-2-2   Session Enabled    Session running

OS910-M(config-tdm2)#
--------------------------------------------------------------------------
```

### Viewing Information about a Specific Session

To view configuration and status information on a session, invoke the command:

**show session detail NAME**

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

Example 1

This example shows a Layer 2 configuration for a session.+

```
OS910-M(config-tdm2)# show session detail s1

                CONFIGURATION

Item                          :  Value
------------------------------:  ---------
Session mode                  :  Enable
Header type                   :  CESoETH
Local ECID                    :  100
Target ECID                   :  100
OOS Local ECID                :  35
OOS Target ECID               :  35
Target MAC                    :  00:12:72:00:5e:54
Payload length (frames)       :  8
Jitter maximum level (ms)     :  5
VLAN enable                   :  Enable
VLAN-ID                       :  100
VLAN priority (VPT)           :  5
MPLS enable                   :  Disable
RTP  enable                   :  Disable
Transport emulation type      :  Unstructured
Session bandwidth (in Kbps)   :  2288
```

```
Payload suppresion            :  Disable
TDM port                      :  P2
Time Slots                    :  1-32

                STATUS/STATISTICS

Item                               :  Status/Value
-----------------------------------:  ---------
Clocking mode                      :  RECOVERY
Eth to TDM direction               :  DOWN
TDM to Eth direction               :  DOWN
PSN Rx status                      :  LOPS
PSN Tx status                      :  UP + L-bit Tx On + R-bit Tx On
Current jitter buffer delay (ms)   :  -
Jitter maximum level (ms)          :  -
Jitter minimum level (ms)          :  -
Valid Eth packets per sec          :  0
Handled Eth packets                :  0
Late Eth packets                   :  0
Lost Eth packets                   :  0
Packets per seconds                :  1000
Packets with L-bit                 :  0
Packets with R-bit                 :  0
Underrun Eth packets               :  17957
Overrun Eth packets                :  0
Malformed packets counter          :  0
Duplicate Eth packets              :  0
Missing Eth packets                :  0
```

Example 2

This example shows a Layer 3 configuration for a session.

```
OS910-M(config-tdm2)# show session detail s3

                CONFIGURATION

Item                          :  Value
------------------------------:  ---------
Session mode                  :  Enable
Header type                   :  SAToP
Local  UDP-port               :  300
Target UDP-port               :  300
IP TOS                        :  184
OOS Local  UDP-port           :  49157
OOS Target UDP-port           :  49157
Local IP address              :  192.168.4.2
Target IP address             :  192.168.1.2
Payload length (frames)       :  8
Jitter maximum level (ms)     :  5
VLAN enable                   :  Enable
VLAN-ID                       :  10
VLAN priority (VPT)           :  6
MPLS enable                   :  Disable
RTP  enable                   :  Disable
Transport emulation type      :  Unstructured
Session bandwidth (in Kbps)   :  2480
Payload suppresion            :  Disable
TDM port                      :  P4
Time Slots                    :  1-32

                STATUS/STATISTICS

Item                               :  Status/Value
-----------------------------------:  ---------
Clocking mode                      :  RECOVERY
Eth to TDM direction               :  UP
TDM to Eth direction               :  UP
PSN Rx status                      :  UP
PSN Tx status                      :  UP
Current jitter buffer delay (ms)   :  4.496
Jitter maximum level (ms)          :  5.0
Jitter minimum level (ms)          :  3.988
```

```
Valid Eth packets per sec          :  100
Handled Eth packets                :  55767670
Late Eth packets                   :  0
Lost Eth packets                   :  0
Packets per seconds                :  1000
Packets with L-bit                 :  0
Packets with R-bit                 :  0
Underrun Eth packets               :  14526
Overrun Eth packets                :  0
Malformed packets counter          :  0
Duplicate Eth packets              :  0
Missing Eth packets                :  0
```

### Viewing only Configuration Information about a Specific Session

To view only configuration information on a session, invoke the command:

**show session detail NAME config**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

Example

```
OS910-M(config-tdm2)# show session detail s02 config

CONFIGURATION

Item                            :  Value
------------------------------:  ---------
Session mode                    :  Enable
Header type                     :  CESoETH
Local ECID                      :  34
Target ECID                     :  34
Target MAC                      :  00:12:72:00:5e:54
Layer 2 support mode            :  VLAN
Payload length (frames)         :  8
Jitter maximum level (ms)       :  5
VLAN enable                     :  Disable
MPLS enable                     :  Disable
RTP  enable                     :  Disable
Transport emulation type        :  Unstructured
Session bandwidth (in Kbps)     :  2256
Payload suppresion              :  Disable
Port                            :  1
Time Slots                      :  1-32
OS910-M(config-tdm2)#
```

### Viewing only Status Information about a Session

To view only status information on a session, invoke the command:

**show session detail NAME status**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

Example

```
OS910-M(config-tdm2)# show session detail s02 status

STATUS/STATISTICS

Item                                :  Status/Value
-----------------------------------:  ---------
Clocking mode                       :  LINE1
Eth to TDM direction                :  UP
TDM to Eth direction                :  UP
Current jitter buffer delay (ms)    :  4.492
Jitter maximum level (ms)           :  4.996
Jitter minimum level (ms)           :  3.996
Valid Eth packets per sec           :  100
Handled Eth packets                 :  229302
Late Eth packets                    :  0
Lost Eth packets                    :  0
Packets per seconds                 :  1000
Underrun Eth packets                :  406
Overrun Eth packets                 :  0
Malformed packets counter           :  0
Duplicate Eth packets               :  0
OS910-M(config-tdm2)#
```

### Viewing the Default Configuration for a Session

To view the default configuration for a session, invoke the command:

**`show session detail NAME default-cfg`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

Example

```
OS910-M(config-tdm2)# show session detail  s02 default-cfg

Items                          Default values
----------------------------- :  -----
Header type                    :  SAToP
Local  UDP-port/ECID           :  49152
Target UDP-port/ECID           :  49152
IP TOS                         :  0x2e
Target IP address              :  169.254.01.101
Payload length (frames)        :  8
Jitter maximum level (ms)      :  5
Target MAC                     :  00.00.00.00.00.00
VLAN enable                    :  Disable
MPLS enable                    :  Disable
RTP  enable                    :  Disable
Transport emulation type       :  Unstructured
Payload suppresion             :  Disable
OS910-M(config-tdm2)#
```

# Configuration Example 1

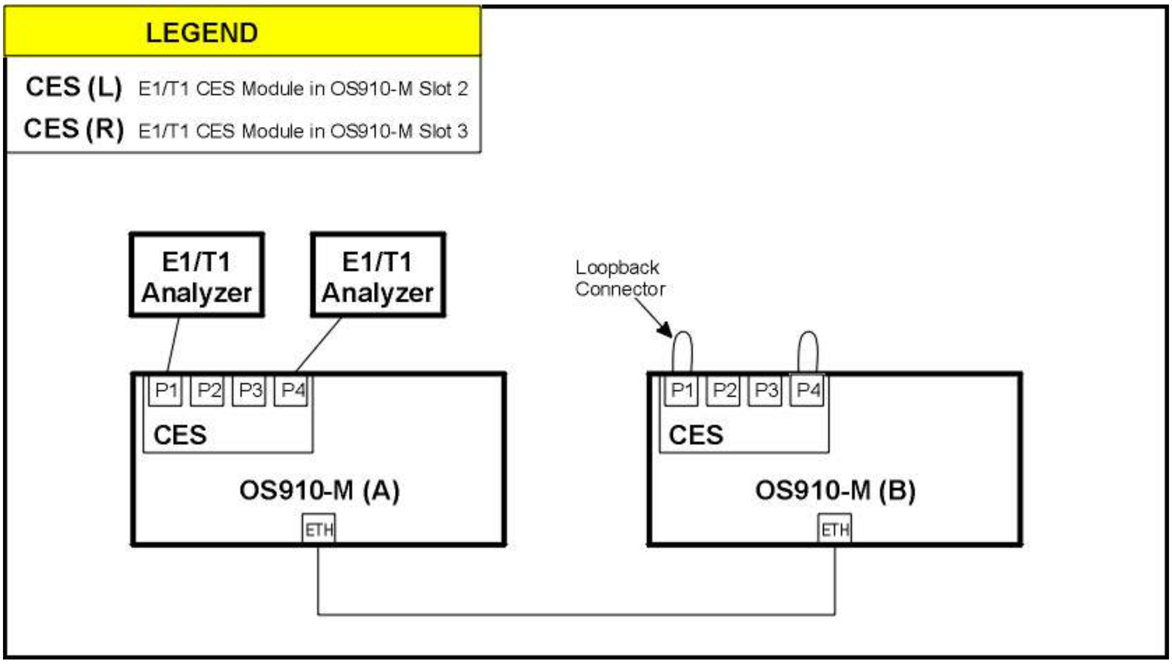
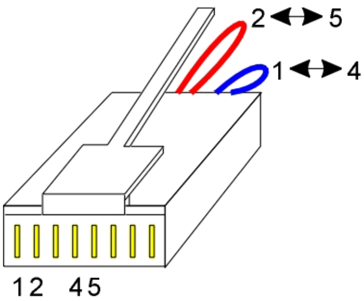



**Figure 63: Interconnection for Layer-3 Traffic and using Internal Clock**

In the above setup:

- Three sessions are defined on E1 ports P1, P2, P4 on OS910-M (A) as well as on OS910-M (B)
- Layer-3 protocol is used for circuit emulation
- Unstructured pseudowire is used on port P1 and P2 while structured pseudowire is used on port P4
- Both E1/T1 CES modules are on the same subnet. As a CES transport interface, a VLAN interface (**`vif6`**) is configured (on each module, and with the same subnet mask) to enable internal switching.
- The IP modules addresses belong to the subnet configured on **`vif6`**.
- CES (L) in OS910-M (A) is set to use its **`internal`** clock (for **`clock mode`**).
- CES (L) in OS910-M (B) is set to use attempt clock recovery in Single-Recovery-Clock mode (using the command **`recovery-clock independent-domain-cfg single`**)
- The Transmit Clock used on OS910-M (B) ports P1 and P4 is recovered from session **`s02`**.
- On Ports P1 and P4, pins are shorted as follows: 1 ←→ 4, 2←→ 5. This can be done by inserting an RJ45 male connector whose wiring is shown below:




The following three routes between OS910-M (A) and OS910-M (B) are defined:

Route 1

**`P1`** on OS910-M (A) ←→ **`s02`** on OS910-M (A) ←→ Ethernet VLAN interface **`vif6`** ←→ **`s02`** on OS910-M (B) ←→ **`P1`** on OS910-M (B).

Route 2

**`P2`** on OS910-M (A) ←→ **`s03`** on OS910-M (A) ←→ Ethernet VLAN interface **`vif6`** ←→ **`s03`** on OS910-M (B) ←→ **`P2`** on OS910-M (B).

Route 3

**`P4`** on OS910-M (A) ←→ **`s04`** on OS910-M (A) ←→ Ethernet VLAN interface **`vif6`** ←→ **`s04`** on OS910-M (B) ←→ **`P4`** on OS910-M (B).

The following session parameter values on OS910-M (A) and on OS910-M (B) must be the same: Header protocol, Timeslots (for structured pseudowire), UDP local and target ports, Target and Source IP. E1/T1 port numbers, however, may be different.

E1/T1 Analyzer 1 and 2 clock source can be from the E1/T1 CES Module or the analyzer itself.

**OS910-M (A) Configuration**

The sequence of CLI commands to be invoked to implement the required configuration for OS910-M (A) is shown below.

```
OS910-M# write terminal
Building configuration

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.11/24
 ports 6
!
dhcp
 enable
!
tdm 2
clock mode internal
module-ip  60.1.1.4/24  interface vif6
 port 4 transport-emulation-type struct
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.2
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
 session s03 description SESSiON-1-2
 session s03 port 2
 session s03 header-proto l3 target-ip 60.1.1.2
 session s03 local-udp-port 49155
 session s03 target-udp-port 49155
 session s04 description SESSiON-3-1
 session s04 port 4 timeslots 2-10
 session s04 header-proto l3 target-ip 60.1.1.2
 session s04 local-udp-port 49156
 session s04 target-udp-port 49156
!
OS910-M#
```

**OS910-M (B) Configuration**

The sequence of CLI commands to be invoked to implement the required configuration for OS910-M (B) is shown below.

```
OS910-M# write terminal
Building configuration

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.1/24
 ports 6
!
dhcp
 enable
!
tdm 2
 clock mode recovery
 module-ip 60.1.1.2/24 interface vif6
 port 4 transport-emulation-type struct
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.4
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
 session s03description SESSiON-2-1
 session s03 port 2
 session s03 header-proto l3 target-ip 60.1.1.4
 session s03 local-udp-port 49155
 session s03 target-udp-port 49155
 session s04 description SESSiON-3-1
 session s04 port 4 timeslots 2-10
 session s04 header-proto l3 target-ip 60.1.1.4
 session s04 local-udp-port 49156
 session s04 target-udp-port 49156
recovery-clock session s02 controller 1
!
```

# Configuration Example 2

The setup & configuration is the same as in the *Configuration Example 1*, page *658* except for the following differences:

- *Multiple-Recovery-Clocks mode* instead of *Single-Recovery-Clock mode* is set on OS910-M (B). Transmit Clock used on port **P1** is recovered from session **s02**, while Transmit Clock used on port **P4** of OS910-M (B) is recovered from session **s04**.
- The clock configurations are as follows:
  E1/T1 Analyzer 1 and 2 clock source can be from the E1/T1 CES Module or the analyzer itself.
  OS910-M (A): Clock mode is **loopback**
  OS910-M (B): Clock mode is **recovery**; Recovery clock mode is **multiple**.

## OS910-M (A) Configuration

```
OS910-M# write terminal
Building configuration

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.11/24
 ports 6
!
dhcp
 enable
!
tdm 2
 clock mode loopback 1
 clock mode loopback 2
 clock mode loopback 3
 clock mode loopback 4
 module-ip 60.1.1.4/24 interface vif6
 port 4 transport-emulation-type struct
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.2
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
 session s03 description SESSiON-1-2
 session s03 port 2
 session s03 header-proto l3 target-ip 60.1.1.2
 session s03 local-udp-port 49155
 session s03 target-udp-port 49155
 session s04 description SESSiON-3-1
 session s04 port 4 timeslots 2-10
 session s04 header-proto l3 target-ip 60.1.1.2
 session s04 local-udp-port 49156
 session s04 target-udp-port 49156
!
OS910-M#
```

## OS910-M (B) Configuration

```
OS910-M# write terminal
Building configuration.

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.1/24
 ports 6
!
dhcp
 enable
!
tdm 2
 clock mode recovery 1
 clock mode recovery 2
 clock mode recovery 3
 clock mode recovery 4
 module-ip 60.1.1.2/24 interface vif6
 port 4 transport-emulation-type struct
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.4
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
 session s03 description SESSiON-2-1
 session s03 port 2
 session s03 header-proto l3 target-ip 60.1.1.4
 session s03 local-udp-port 49155
 session s03 target-udp-port 49155
 session s04 description SESSiON-3-1
 session s04 port 3 timeslots 2-10
 session s04 header-proto l3 target-ip 60.1.1.4
 session s04 local-udp-port 49156
 session s04 target-udp-port 49156
recovery-clock session s02 controller 1
 recovery-clock session s04 controller 1
!
```

# Configuration Example 3

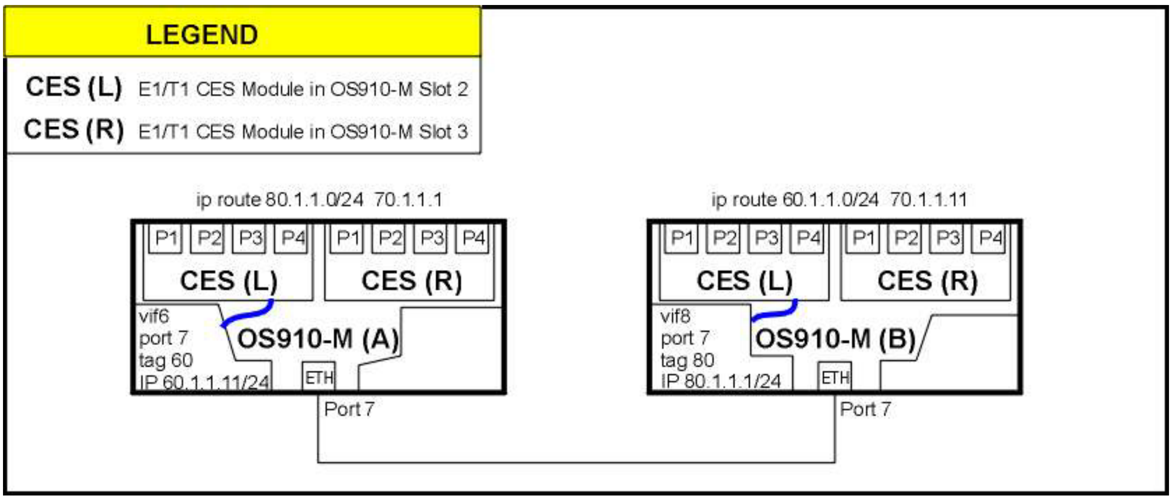



**Figure 64: Interconnection for Layer-3 Traffic and using Different Subnets**

In the above setup:

– The E1/T1 CES Modules in the OS910-M (A) and OS910-M (B) have source IP addresses of different subnets.

– The subnet used for Ethernet connectivity (CES transport) between OS910-M (A) and OS910-M (B) is different from those of the E1/T1 CES Modules. This means that the E1/T1 CES Module in OS910-M (A) and in OS910-M (B) need to route traffic between them (using a static route).

  If a subnet (VLAN interface) is to be used only by the E1/T1 CES Module in OS910-M (A) or in OS910-M (B), it is enough to configure the tag and IP address for the VLAN interface. That is, there is no need to include ports in the VLAN interface.

The Layer-3 traffic route between the E1/T1 CES Module in OS910-M (A) and the E1/T1 CES Module in OS910-M (B) is as follows:

E1/T1 CES Module in OS910-M (A) (IP 60.1.1.4) ←→ OS910-M (A) VLAN Interface (IP 60.1.1.11/24) ←→ OS910-M (A) subnet (IP 70.1.1.11/24) ←→ OS910-M (B) subnet (IP 70.1.1.1/24) ←→ OS910-M (B) VLAN Interface (IP 80.1.1.1/24) ←→ E1/T1 CES Module in OS910-M (B) (IP 80.1.1.2).

**OS910-M (A) Configuration**

```
OS910-M# write terminal
Building configuration

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.11/24
!
interface vlan vif7
 tag 70
 ip 70.1.1.11/24
 ports 7
!
ip route 80.1.1.0/24 70.1.1.1
!
dhcp
 enable
!
tdm 2
 clock mode internal
 module-ip 60.1.1.4/24 interface vif6
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 80.1.1.2
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
!
OS910-M#
```

## OS910-M (B) Configuration

```
OS910-M# write terminal
Building configuration

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif7
 tag 70
 ip 70.1.1.1/24
 ports 7
!
interface vlan vif8
 tag 80
 ip 80.1.1.1/24
!
ip route 60.1.1.0/24 70.1.1.11
!
dhcp
 enable
!
tdm 2
 clock mode recovery
 module-ip 80.1.1.2/24 interface vif80
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.4
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
recovery-clock session s02 controller 1
!
OS910-M#
```

# Configuration Example 4

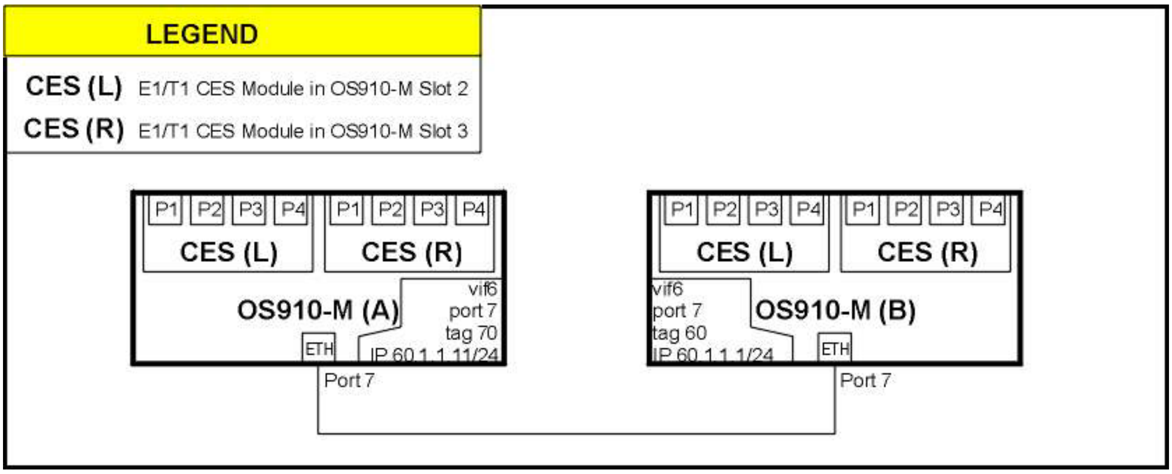



**Figure 65: Interconnection for Layer-2 Traffic and using IP and DHCP**

In the above setup:

- Layer-2 protocol is used.
- The interface used for CES transport is an IP VLAN interface and source IP address is defined for the E1/T1 CES Modules.

To get the MAC address of the partner E1/T1 CES Module invoke the following command on the partner CLI:

**`show module mac-addr`**

## OS910-M (A) Configuration

```
!
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 70
 ip 60.1.1.11/24
 ports 7
!
dhcp
 enable
!
tdm 2
 clock mode internal
 module-ip 60.1.1.4/24 interface vif6
 session s03 description SESSiON-1-2
 session s03 port 1
 session s03 header-proto l2 target-mac 00:12:72:00:5e:58
 session s03 local-ecid 34
 session s03 target-ecid 34
!
#
```

## OS910-M (B) Configuration

```
!
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.1/24
 ports 7
!
dhcp
 enable
!
tdm 2
 clock mode recovery
 module-ip 60.1.1.2/24 interface  vif6
 session s03 description SESSiON--2
 session s03 port 1
 session s03 header-proto l2 target-mac 00:12:72:00:5e:54
 session s03 local-ecid 34
 session s03 target-ecid 34
 recovery-clock session s03 controller 1
!
```

# Configuration Example 5

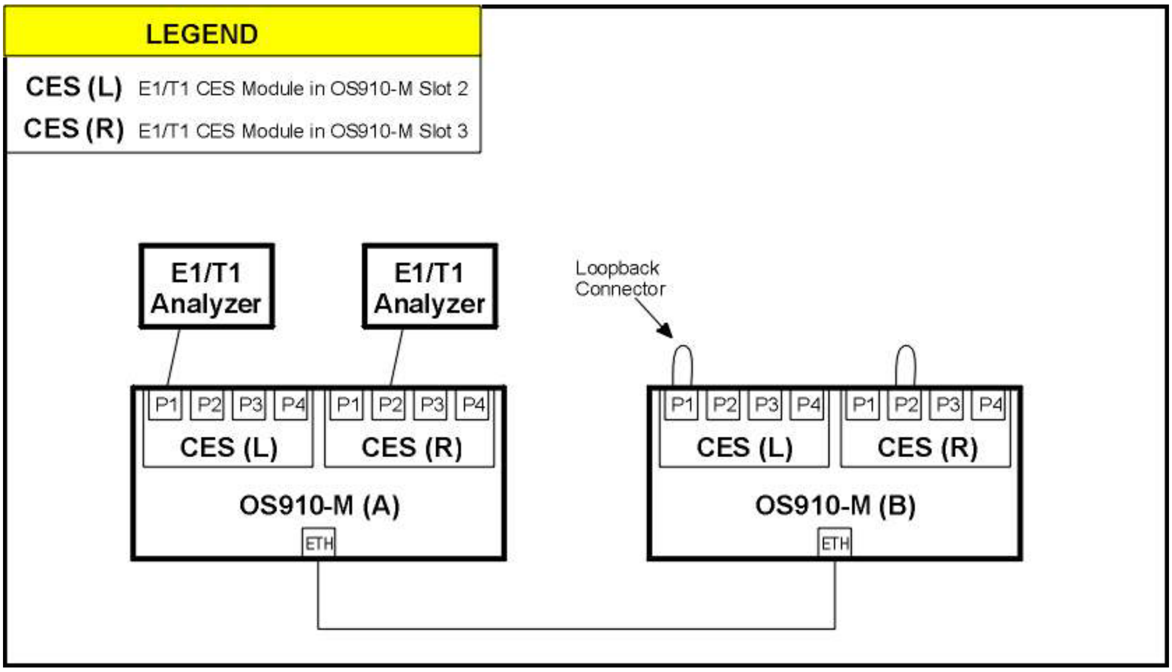
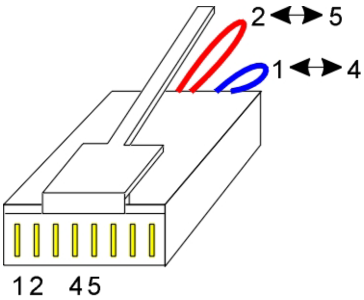



**Figure 66: Interconnection using Clock Exportation**

In the above setup:

- Two sessions are defined, one on E1 port 1 (P1) of the *left* E1/T1 CES Module (CES (L)), the other on E1 port 2 (P2) of the *right* E1/T1 CES Module (CES (R)) on OS910-M (A) as well as on OS910-M (B).
- Clock exported to the neighbor E1/T1 CES Module.
- CES (L) in OS910-M (A): Clock mode is **`line1`**.
- CES (R) in OS910-M (A): Clock mode is **`external`** (received from the neighbor CES (L)).
- CES(L)-OS910-M (B): Clock mode is **`recovery`**. Adaptive clock from pseudowire session.
- CES(R)-OS910-M (B): Clock mode is **`external`** (received from the neighbor CES (L) in OS910-M (B))
- On Ports P1 and P2, pins are shorted as follows: 1 ←→ 4, 2←→ 5. This can be done by inserting an RJ45 male connector whose wiring is shown below:



## OS910-M (A) Configuration

```
OS910-M# write terminal
Building configuration...

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.1/24
 ports 6
!
dhcp
 enable
!
tdm 2
 clock mode line1
 module-ip 60.1.1.2/24 interface vif6
 clock output recovered
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.12
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
!
tdm 3
 clock mode external
 module-ip 60.1.1.3/24 interface vif6
 clock input-ext other-slot-recovered
 session s03 description SESSiON-2-1
 session s03 port 2
 session s03 header-proto l3 target-ip 60.1.1.13
 session s03 local-udp-port 49153
 session s03 target-udp-port 49153
!
#OS910-M#
```

## OS910-M (B) Configuration

```
OS910-M# write terminal
Building configuration...

Current configuration:
! version main-d1550-10-11-06
!
interface vlan vif6
 tag 60
 ip 60.1.1.11/24
 ports 6
!
dhcp
 enable
!
tdm 2
 clock mode recovery
 module-ip 60.1.1.12/24 interface vif6
 clock output recovered
 session s02 description SESSiON-1-1
 session s02 port 1
 session s02 header-proto l3 target-ip 60.1.1.2
 session s02 local-udp-port 49152
 session s02 target-udp-port 49152
 session s02 vlan 60 vpt 6
recovery-clock session  s02  controller 1
!
tdm 3
 clock mode external
 module-ip 60.1.1.13/24 interface vif6
 clock input-ext other-slot-recovered
 session s03 description SESSiON-2-1
 session s03 port 2
 session s03 header-proto l3 target-ip 60.1.1.13
 session s03 local-udp-port 49153
 session s03 target-udp-port 49153
 session s03 vlan 60 vpt 6
!
```

# Configuration Example 6

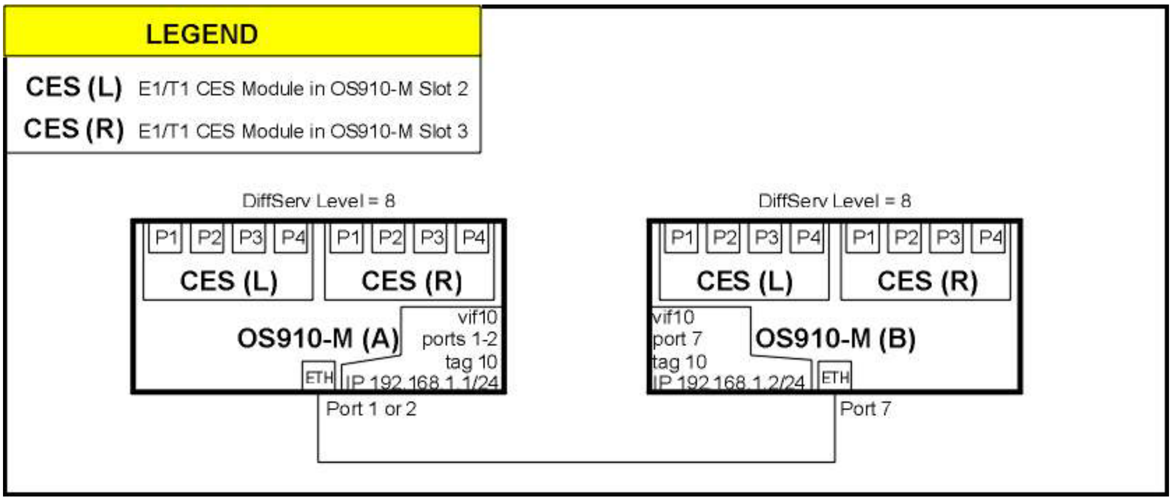



**Figure 67: Interconnection using High DiffServ Level**

In the above setup:

– A high DiffServ level is set for the TDM traffic. The high DiffServ level is useful when TDM and data traffic between two switches (OS910-Ms) pass through the same VLAN interface (**`vif10`**).

– CES (L) in OS910-M (A): Clock mode is **`line1`**, Clock exportation is **`recovered`**, Diffserv Level is highest (8)

– CES(R)-OS910-M (A): Clock mode is **`external`**, Clock selected from neighbor slot (using the command **`clock input-ext other-slot-recovered`**), Diffserv Level is highest (8)

– CES (L) in OS910-M (B): Clock mode is **`line1`**, Clock mode is **`recovery`**, Diffserv Level is highest (8)

The DSCP value = 46 corresponds to ToS value=184.

**OS910-M (A) Configuration**

```
access-list extended acl1
 rule 10
  dscp eq 0xb8
  action mark sl 8
!
!
interface vlan vif10
 tag 10
 ip 192.168.1.1/24
 ports 1-2
 access-group acl1 1
!
dhcp
 enable
!
tdm 2
 clock mode line1
 module-ip 192.168.1.10/24 interface vif10
 clock output recovered
 ces traffic egress sl 8
 session s01 description s01
 session s01 port 1
 session s01 header-proto l3 target-ip 192.168.1.30
 session s01 ip-tos 184
 session s01 local-udp-port 49152
 session s01 target-udp-port 49152
!
tdm 3
 clock mode external
 module-ip 192.168.1.20/24 interface vif10
 clock input-ext other-slot-recovered
 ces traffic egress sl 8
 session s02 description s02
 session s02 port 4
 session s02 header-proto l3 target-ip 192.168.1.40
 session s02 ip-tos 184
 session s02 local-udp-port 57343
 session s02 target-udp-port 57343
```

| | **Note** |
|---|---|
| | 0xb8 (= decimal 184) is the highest priority value for ToS.<br>0x0 (= decimal 0) is the lowest priority value for ToS, and is the default value.<br>For SL mapping details, refer to ***Chapter 14:*** *Quality of Service (QoS)*, page *281*. |

## OS910-M (B) Configuration

```
access-list extended acl1
 rule 10
  dscp eq 0xb8
  action mark sl 8
!
port sl 8 21,23
!
interface vlan vif10
 tag 10
 ip 192.168.1.2/24
 ports 1-2
 access-group acl1 1
!
dhcp
 enable
!
tdm 2
 clock mode recovery
 module-ip 192.168.1.30/24 interface vif10
 clock output recovered
 ces traffic egress sl 8
 session s01 description s01
 session s01 port 4
 session s01 header-proto l3 target-ip 192.168.1.10
 session s01 ip-tos 184
 session s01 local-udp-port 49152
 session s01 target-udp-port 49152
 session s01 vlan 10 vpt 6
recovery-clock session s01 controller 1
!
tdm 3
 clock mode external
 module-ip 192.168.1.40/24 interface vif10
 clock input-ext other-slot-recovered
 ces traffic egress sl 8
 session s02 description s02
 session s02 port 4
 session s02 header-proto l3 target-ip 192.168.1.20
 session s02 ip-tos 184
 session s02 local-udp-port 57343
 session s02 target-udp-port 5734
 session s02 vlan 10 vpt 6
```

# Alarms

## List

The list of all alarms about the E1/T1 CES module that can be received is given below.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Link UP.
HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Link DOWN.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm RCV-FE-LOF.
*Denotation*: Far End sending Lost-Of-Frame.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm XMT-FE-LOF.
*Denotation*: Near End sending Lost-Of-Frame indication.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm RCV-AIS.
*Denotation*: Far End sending Alarm-Indication-Signal (AIS).

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm XMT-AIS.
*Denotation*: Near End sending AIS.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm LOF.
*Denotation*: Near End Lost-Of-Frame.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm LOS.
*Denotation*: Near End Lost-Of-Signal.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm LOOPBACK.
*Denotation*: Near End is Looped.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm RCV-TEST-CODE.
*Denotation*: Near End detects a test code.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm OTHER-FAILURE.
*Denotation*: Any line status not defined here.

HH:MM:SS E1 ALARM: slot SLOT-NUM, port E1-PORT-NUM, msg: Alarm cleared.

HH:MM:SS E1 ALARM: slot SLOT-NUM, clock CLOCK-NAME, msg: mode changed to Free Running.
HH:MM:SS E1 ALARM: slot SLOT-NUM, clock CLOCK-NAME, msg: mode changed to Normal.

HH:MM:SS E1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: jitter-buffer Underflow.
*Denotation*: No packets are present in the jitter buffer.

HH:MM:SS E1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: jitter-buffer Overflow.
*Denotation*: Jitter buffer cannot accommodate newly arrived packets.

HH:MM:SS E1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: jitter-buffer Normal.

HH:MM:SS E1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: R-bit detect.
*Denotation*: Remote packet loss (on ETH) is indicated by reception of packets with their R bit set.

HH:MM:SS E1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: excessive loss.
*Denotation*: Excessive packet loss rate is detected.

HH:MM:SS E1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: no defects.

Examples:
14:48:05 E1 ALARM: slot 2, port 1, msg: Link DOWN.
14:58:04 E1 ALARM: slot 2, clock C1, msg: mode changed to Normal.
14:47:54 E1 ALARM: slot 2, sessions s1, msg: jitter-buffer Normal.

## Indication

### Enabling

To enable indication of alarms, invoke the command:

```
alarm
```

### Disabling

To disable indication of alarms, invoke the command:

```
no alarm
```

## Target

To specify alarm target(s), invoke the command:

```
alarms target (all|cli|console|log|snmp)
```

where,

**all**: All targets
**cli**: CLI (TELNET/SSH) sessions
**console**: System console
**log**: System log
**snmp**: SNMP manager

To exlude alarm target to use the CLI-command:

```
no alarms target (all|cli|console|log|snmp)
```

where,

**all**: All targets
**cli**: CLI (TELNET/SSH) sessions
**console**: System console
**log**: System log
**snmp**: SNMP manager

# Upgrading/Downloading

## Requirements

- Connection of the OS910-M to an external FTP server having the EM9-CES image (operative firmware)
- Connection of a craft terminal[88] *or* TELNET station to the OS910-M. (The baud rate of the craft terminal/TELNET station must be 9600 baud.)

## Procedure

The procedure for upgrading/downloading an EM9-CES image is as follows:

1. From **configure terminal** mode enter **tdm** mode by invoking the command:

   **tdm SLOT-NUM**

   where,

   **SLOT-NUM**: Number of the slot hosting the EM9-CES.

2. Copy the EM9-CES image from the FTP server to the OS910-M by invoking the command:

   **copy tdm-ver ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]**

   where,

   **FTP-SERVER**: Host name or IP address of the FTP server containing the image to be downloaded.

   **REMOTE-DIR**: Full path to the directory containing the image on the FTP server.

   **REMOTE-FILENAME**: Name of the image file in the directory

   **USERNAME**: Name of user authorized to access the FTP server.

   **PASSWORD**: Password for accessing the FTP server.

Example

```
OS910-M# configure terminal
OS910-M(config)# tdm 2
OS910-M(config-tdm2)# copy tdm-ver ftp 192.32.32.32 versions CMX1624-v18.bin Tarzan
MyPassword

sudo /usr/local/nbase/bin/copy_tdmver.sh 192.32.32.32 versions CMX1624-v18.bin Tarzan
MyPassword
Check route to 192.32.32.32
Netmask = 255.255.255.0
FTP file versions/CMX1624-v18.bin from 192.32.32.32 user Tarzan password MyPassword ...
FTP Succeed
OS910-M(config-tdm2)#
```

In the above example:

Number '2' in the prompt 'OS910-M(config-tdm2)#' signifies that the E1/T1 CES module to which the image will be downloaded is in slot 2 of the OS910-M.

To verify that the E1/T1 CES E1/T1 CES module image has been copied from the FTP server to the OS910-M, invoke the command:

**show module firmware-download-info**

[88] Asynchronous ASCII terminal, e.g., *VT100* terminal capable of operating with the Serial/RS-232 protocol

Example

```
OS910-M(config-tdm2)# show module firmware-download-info

SW version file of TDM module is stored in the switch : CMX1624-v18.bin
SW version is running on the TDM module               : CMX1624-R01.00.00_D017.bin
TFTP server IP                                        : 0.0.0.0
OS910-M(config-tdm2)#
```

In the above example:

'`SW version file of TDM module is stored in the switch`' signifies that the image has been copied to the OS910-M. '`CMX1624-v18.bin`' is the name of the copied image file.

'`SW version is running on the TDM module ...`' signifies the image version currently running.

3. Copy the EM9-CES image from the OS910-M to the EM9-CES Flash memory by invoking the command:

   **`sw-dnld FILENAME`**

   where,

   **`FILENAME`**: Name of the image file

Example

```
OS910-M(config-tdm2)# sw-dnld CMX1624-v18.bin
The download process of the TDM module (slot 2) started.
......................................................
......................................................
TDM module restarted after downloaded.
The TDM module download process is finished.

OS910-M(config-tdm2)#
```

At the end of the download process the EM9-CES is automatically reset and run with the new image.

4. Clear the EM9-CES image from the OS910-M by invoking the command:

   **`remove firmware-download-file`**

Example

```
OS910-M(config-tdm2)#remove firmware-download-file
OS910-M(config-tdm2)#
```

# Product Specification

| | |
|---|---|
| **E1 Port** | |
| Purpose | Connection to E1 voice lines |
| Data Rate | 2.048 Mbps |
| Line Code | HDB3, AMI |
| Receive Level | 0 to –43 dB, 0 to –12 dB |
| Connector | RJ45 female 8-pin shielded connector |
| **T1 Port** | |
| Purpose | Connection to T1 voice lines |
| Data Rate | 1.544 Mbps |
| Line Code | B8ZS, AMI |
| Receive Level | 0 to –36 dB, 0 to –15 dB |
| Connector | RJ45 female 8-pin shielded connector |
| **External Clock Port** | |
| Purpose | Connection to external clock source |
| Connector Type | SMB jack |
| **Cabling** | |
| ***1000Base-T*** | |
| Cable Type: | Category 5, 4-pair, UTP or STP |
| Cable Impedance (max) | 100 Ω |
| Cable Length (max): | 100 m (330 ft) |
| Connector Type: | RJ45, male, 8-pin, shielded |
| ***1000Base-X*** | |
| Cable Type: | Duplex, Multimode, 1310 nm, up to 2 km |
| Cable Length (max): | 100 m (330 ft) |
| Connector Type: | RJ45, male, 8-pin, shielded |
| ***External Clock*** | |
| Cable Type | RG-174 |
| Cable Impedance | 50 Ω |
| Cable Length (max) | 5 m (16.5 ft) |
| Cable Connector | SMB male |
| **Protocols** | |
| Circuit Emulation | SAToP, CESoPSN, CESoETH MEF-8/3 |
| TDM Traffic | SAToP structure agnostic |
| | CESoPSN structured & unstructured |
| | CESoETH structured & unstructured |

| | |
|---|---|
| | Fractional DS0 granularity |
| Signaling | CAS relay as per the CES standards |
| Clocking | Adaptive |
| | Internal, external, loopback |
| **Standards** | |
| ***E1*** | ITU-T Rec. G.703, G.704, G.823 |
| ***T1*** | AT&T TR-6241/ITU-T Rec. G.703, G.704, ANSI T1.403, G.824 |
| **Framing** | |
| ***E1*** | CRC4 MF, CAS MF |
| ***T1*** | D4 (SF), ESF |

# Chapter 39: STM-1/OC3 CES Module

## Applicability

The STM-1/OC3 CES module (EM9-CES-OC3) applies to OS910-M only.

## Terminology

**SDH:** European standardized multiplexing protocol that transfers multiple digital bit streams over optical fiber.

**SONET:** American standardized multiplexing protocol that transfers multiple digital bit streams over optical fiber.

**STM-1:** European SDH digital transmission line with data speeds of up to 155.52 Mbps (payload: 148.608 Mbit/s; overhead: 6.912 Mbps, including path overhead) over fiberoptic networks.

**OC3:** American SONET digital transmission line with data speeds of up to 155.52 Mbps (payload: 148.608 Mbps; overhead: 6.912 Mbps, including path overhead) over fiberoptic networks. Depending on the system, OC3 is also known as STS-3 (electrical level).

**E1:** European digital transmission format of *thirty-two* 8-bit voice channels (time slots) together having a total bandwidth of 2.048 Mbps.

**T1:** American digital Transmission format of *twenty-four* 8-bit voice channels (time slots) together having a total bandwidth of 1.544 Mbps.

**CES:** (**C**ircuit-**E**mulation **S**ervice) Service that emulates *synchronous* circuits (e.g., STM-1 or OC3) over *asynchronous* networks (e.g., Ethernet).

**Pseudowire Network:** An emulated synchronous circuit (e.g., STM-1 or OC3) in a packet-switching network.

**Pseudowire:** Stream of packets (in a pseudowire network) emulating an E1/T1 channel of the STM-1/OC3 CES module.

**Session:** Specification of the pseudowire. The specification includes the following parameters: source STM-1/OC3 CES module port, pseudowire packet format, maximum jitter, header format, address of target STM-1/OC3 CES module, etc.

**Gateway:** A device interfacing networks of different protocols and functioning as a protocol converter in order to provide interoperability of systems interconnected across the networks.

**TDM:** (**T**ime-**D**ivision **M**ultiplexing) A method of placing multiple data streams in a single signal. The segments of each specific stream are time-separated from one another by segments of other streams in a periodic manner. At the receiving end, the segments of each data stream are reassembled using timing.

**PDH:** (Plesiochronous Digital Hierarchy) is a technology used to transport digital data over telecommunications networks whose parts are only nominally synchronized. A PDH circuit is part of a PDH network that provides a service path across the network.

# Overview

## General

The SDH/SONET STM-1/OC3 carrier has a bandwidth of 155.52 Mbps.

Timing for data transmission is provided by a clock source. A clock source consists of the *system clock*[89] and the *service clocks*[90].

The system clock is the STM-1/OC3 interface's line clock.

The service clock is the clock of a single PDH circuit mapped to an E1/T1 channel of the STM-1/OC3 line. The STM-1/OC3 CES module can provide a separate clock for each service (i.e., up to 63 clocks for the 63 E1 services and up to 84 clocks for the T1 services) or a common clock for all the services.

The source of the *system clock* can be selected to be any of the following:

- SDH/SONET line (data)
- Internal (on-board)
- External 1
- External 2

The source of the *service clock* can be selected to be any of the following:

- Local (system). All circuits are timed using the system clock.
- Loopback (SDH/SONET line). Each circuits is timed using its Rx clock.
- Recovery (Ethernet PSN)

The STM-1/OC3 CES module can provide a separate clock for each service or a common clock for all the services.

## Purpose

The STM-1/OC3 CES module is an STM-1/OC3 CES gateway TDM for IP/Ethernet networks.

# Applications

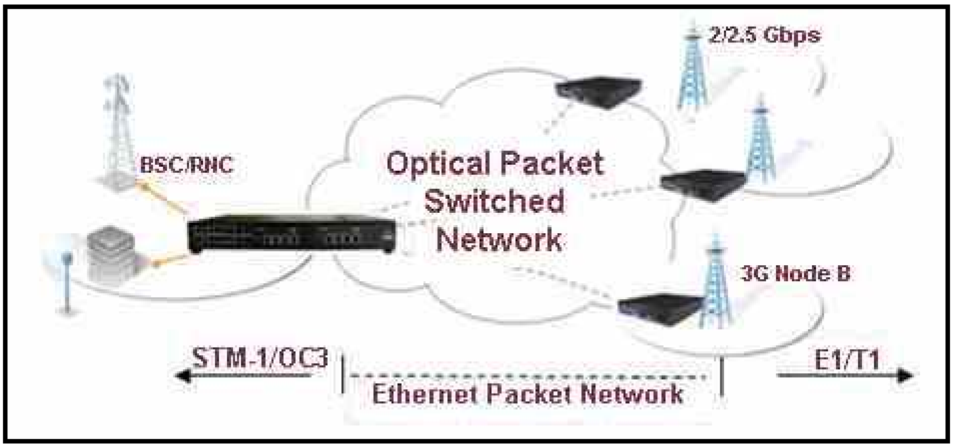



**Figure 68: Mobile Backhaul CES**

[89] On-board clock

[90] E1 or T1 channel clock

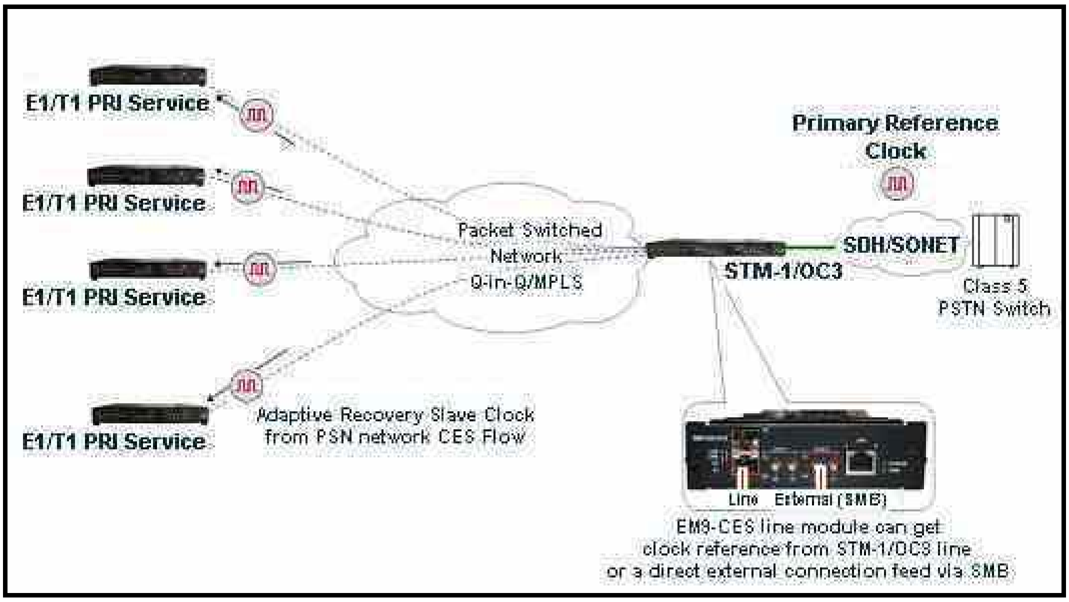



**Figure 69: Telephony PRI CES**

# Network Topology

A typical application of the STM-1/OC3 CES module is in a star topology network.

In the *star* topology one STM-1/OC3 CES module is connected to multiple E1/T1 CES modules over an Ethernet network.

# Layout

## View

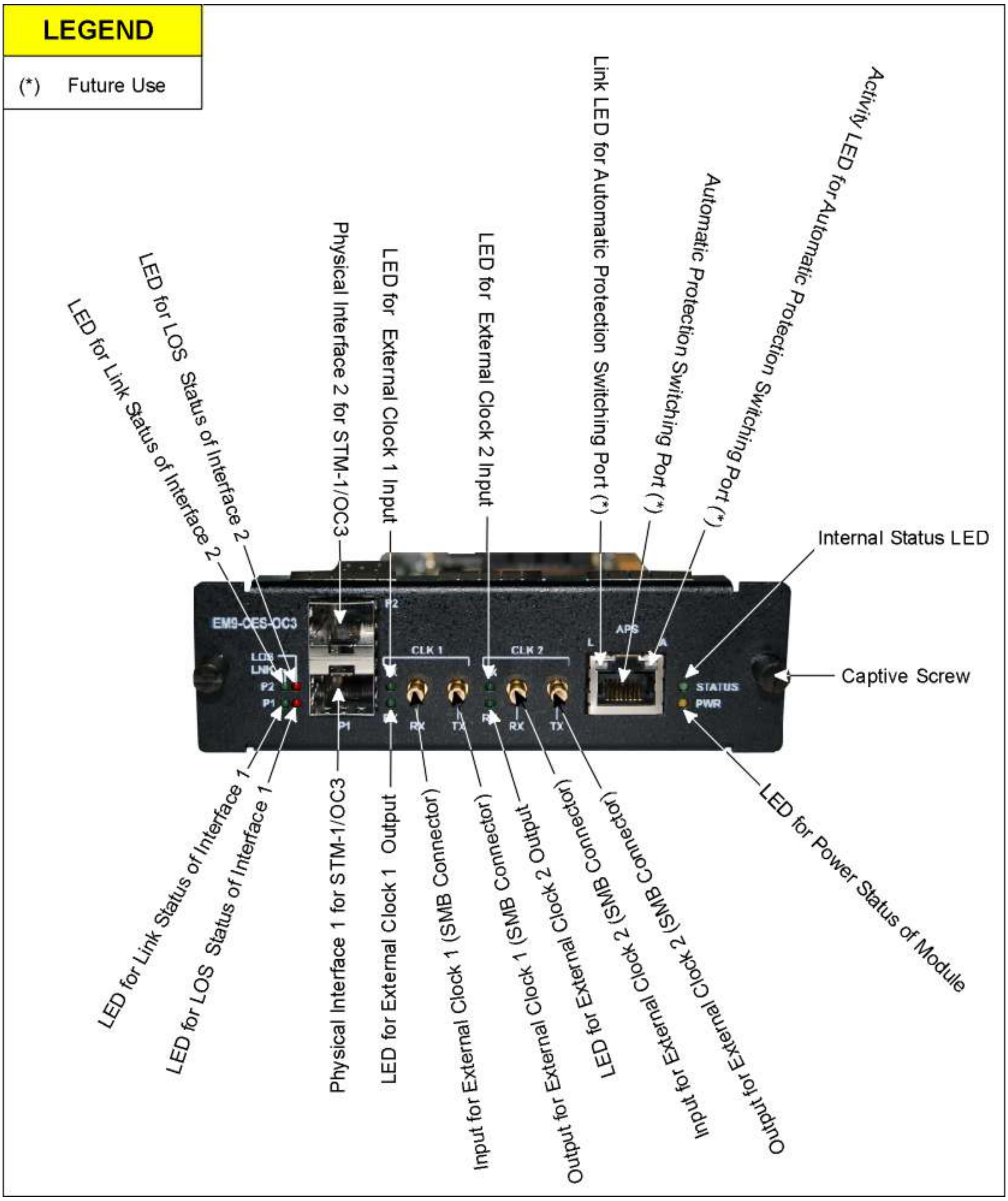



**Figure 70: STM-1/OC3 CES module**

## Ports

### STM-1/OC3 (P1, P2)

Port for STM-1/OC3 Input/Output. Its two SFP interfaces P1 and P2 can be set to function in mutual redundancy mode.

### External Clock 1 Input (CLK 1 RX)

Input for external clock 1.

**External Clock 1 Output (CLK 1 TX)**
Output for external clock 1.

**External Clock 2 Input (CLK 2 RX)**
Input for external clock 2.

**External Clock 2 Output (CLK 2 TX)**
Output for external clock 2.

**Automatic Protection Switching**
For future use. Fixed interface port.

### LEDs

Refer to the section *Monitoring*, page *682*.

## Requirements

- All channels must be either only E1 or only T1.
- 6-inch flat-tip screwdriver (for fastening clock input)
- One OS910-M for housing up to two STM-1/OC3 CES modules
- STM-1/OC3 CES modules (per the network topology)
- For external clock input: RG-174 cable with SMB male connector, up to 5 m (16.5 ft), and having 50 Ω impedance (1 cable per STM-1/OC3 CES module)
- Ethernet cables (per the network topology)
- If an external clock is to be used, its frequency must be one of the following: 8 KHz, 1.544 MHz, 2048 MHz, or 19.44 MHz.

## Mounting

1. Choose slot 2 or 3[91] in the OS910-M into which the STM-1/OC3 CES module is to be inserted.
2. If a Blank Panel is covering the slot, using a philips screwdriver no. 1 remove it by undoing the *two* philips screws.
3. Holding the STM-1/OC3 CES module with the right side up, place the edges of the module's PCB between the left and right rails in the slot and slide it until its panel is level with the front panel of the OS910-M. (This assures that the module's connector is inserted into place.)
4. With a flat-head No.1 screwdriver, fasten the module with the two captive screws that are located on its edges.

## Cabling

1. Connect the STM-1/OC3 line to the physical interface P1 (and to physical interface P2 for redundancy mode) of the STM-1/OC3 CES modules.
2. Optionally, to each STM-1/OC3 module connect one or two external clock sources to the ports CLK 1 RX and CLK 2 RX.
3. Optionally, use the CLK 1 TX and CLK 2 TX ports as clock sources for other devices.
4. Connect the Ethernet ports of the OS910-Ms to Ethernet network.

## Power

Make sure that the OS910-Ms are powered up.

---

[91] Slots 2 and 3 are indicated in *the Figure 2: Layout of OS900* of the OS910-M, page *65*.

# Operation

**Startup**

The STM-1/OC3 CES module becomes fully operational within a few seconds after being powered ON.

**Monitoring**

Operation of the STM-1/OC3 CES module can be monitored by interpreting the status of its LEDs with the aid of *Table 29*, below, or with a management station (e.g., craft terminal, TELNET, UNIX, or Linux station, SSH host, or SNMP NMS).

**Table 32: Front Panel LEDs**

| LED | Status | Significance |
|---|---|---|
| PWR | ON | Power to STM-1/OC3 CES module *OK*. |
| | OFF | Power to STM-1/OC3 CES module *faulty*. |
| STATUS | ON | Internal status of STM-1/OC3 CES module *OK*. |
| | OFF | Internal status of STM-1/OC3 CES module *faulty*. |
| LNK P1 | ON | Link to P1 interface *OK*. |
| | OFF | Link to P1 interface *faulty*. |
| LOS P1 | ON | LOS at P1 interface. |
| | OFF | No LOS at P1 interface. |
| LNK P2 | ON | Link to P2 interface *OK*. |
| | OFF | Link to P2 interface *faulty*. |
| LOS P2 | ON | LOS at P2 interface. |
| | OFF | No LOS at P2 interface. |
| CLK 1 RX | ON | STM-1/OC3 CES module *synchronized* to the external clock at CLK 1 RX port. |
| | BLINKING | External clock at CLK 1 RX port *enabled* but STM-1/OC3 CES module *not synchronized* to the external clock. |
| | OFF | STM-1/OC3 CES module *not synchronized* to the external clock at CLK 1 RX input. |
| CLK 1 TX | ON | External clock at CLK 1 RX input *enabled* at CLK 1 TX output. |
| | OFF | External clock at CLK 1 RX input *disabled* at CLK 1 TX output. |
| CLK 2 RX | ON | STM-1/OC3 CES module *synchronized* to the external clock at CLK 2 RX port. |
| | BLINKING | External clock at CLK 2 RX port *enabled* but STM-1/OC3 CES module *not synchronized* to the external clock. |
| | OFF | STM-1/OC3 CES module *not synchronized* to the external clock at CLK 2 RX input. |
| CLK 2 TX | ON | External clock at CLK 2 RX input *enabled* at CLK 2 TX output. |
| | OFF | External clock at CLK 2 RX input *disabled* at CLK 2 TX output. |
| APS L | Future use | |
| APS A | Future use | |

# Principle of Operation

## Pseudowire Modes

There are two modes in which a pseudowire can be formed:

– Unstructured

– Structured

**Unstructured**

In unstructured mode all E1/T1 channels (timeslots) of the STM-1/OC3 carrier are assigned to one destination. The bit stream is packetized according to the session header and other session parameters and then sent to the Packet-Switching Network (PSN). The packet stream has no discernible channel boundaries or any other signaling information.

**Structured**

In structured mode, all channels or specific channels from an E1/T1 interface can be sent to the destination. The STM-1/OC3 CES module at the receiving end of the pseudowire samples the bit stream on the basis of the type of PCM (whether for STM-1 or OC3) specified in the session. The STM-1/OC3 CES module uses this basis to obtain the signaling information, strips the bit stream of its signaling information, and sends only the data. When necessary it sends a signaling packet stream to indicate change in signaling information.

## TDM over Packet Session

The source and target TDM modules require matching session specifications. According to these specifications, the TDM-over-Packet application divides the STM-1 or OC3 data stream received on the STM-1/OC3 port into pseudowire packets, adds a special header, and transmits the packets via the Ethernet network towards the target STM-1/OC3 CES module. The application at the other end of the pseudowire receives the psedowire packets, removes the header, unpacks the data, and transmits it to the E1/T1 circuit via the E1/T1 ports.

## Packet Header Formats

Packet headers can have any of the following three formats:

- SAToP
- CESoPSN
- CESoETH

**SAToP**

This header format complies with the *IETF PWE3 SAToP* standard for *unstructured* TDM over PSNs. The header requires 62 bytes per packet, including Ethernet, IP, UDP, and RTP headers and the *SAToP* control word.

**CESoPSN**

This header format complies with the *IETF PWE3 CESoPSN* standard for *structured* TDM over PSNs. The header requires 62 bytes per packet, including Ethernet, IP, UDP, and RTP headers and the *CESoPSN* control word.

**CESoETH**

This header format complies with the *MEF 8* specification *Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks*. It supports both *unstructured* and *structured* pseudowires. The header consists of an Ethernet header, an emulation circuit definition (ECID), and a CESoETH control word having a length of 22 bytes.

# Interfaces

## Names

Two VLAN interfaces are reserved for two STM-1/OC3 CES modules in an OS910-M. These VLAN interfaces are TDMS**2L**, and TDMS**3L**. Their relation to configuration, management, and the slots in the OS910-M housing the STM-1/OC3 CES module are shown in *Table 30*, below.

**Table 33: OS910-M-controlled VLAN Interfaces for STM-1/OC3 CES modules**

| | Slot 2 | Slot 3 |
|---|---|---|
| **CES Management** | TDMS2L | TDMS3L |

If no STM-1/OC3 CES module is inserted (sensed) in slot **2** the VLAN interface TDMS2L is not created. The VLAN interface is created automatically when an STM-1/OC3 CES module is inserted in slot **2**.

Similarly, if no STM-1/OC3 CES module is inserted (sensed) in slot **3** the VLAN interface TDMS3L is not created. The VLAN interface is created automatically when an STM-1/OC3 CES module is inserted in slot **3**.

*The user cannot manipulate these interfaces in any other way!*

To view these interfaces:

1. Enter **enable** mode.
2. Invoke the command:
   **show interface**

Example

```
OS910-M# show interface

INTERFACES TABLE

================

Name    M Device        IP                 State MAC               Tag  Ports
--------------------------------------------------------------------------------
TDMS2L.   vif4092       10.10.10.33/28      UP   00:0F:BD:FF:53:B7 4092
TDMS3L.   vif4093       10.10.10.49/28      UP   00:0F:BD:FF:53:B7 4093
vif0      vif0          -                   UP   00:0F:BD:00:53:B7 0001 1,3-4

- 'vif0' is the default forwarding interface.
-  drop-tag is 4094.

OS910-M#
```

The two VLAN interfaces `TDMS2L` and `TDMS3L` are displayed as in the above example when two STM-1/OC3 CES modules are present in the OS910-M.

## Tags

When STM-1/OC3 CES modules are inserted into an OS910-M, VLAN tags are automatically assigned to the VLAN interfaces of the STM-1/OC3 CES modules according to *Table 31*, below. The user cannot assign these VLAN tags to other VLAN interfaces while the STM-1/OC3 CES modules are in the slots.

**Table 34: VLAN Names and Associated VLAN Tags**

| VLAN Names | VLAN Tags |
|---|---|
| TDMS2L | 4092 |
| TDMS3L | 4093 |

## Interface Subnet

The interface subnet 10.10.10.0/24 is reserved for the VLAN interfaces TDMS2L and TDMS3L. During initialization[92] of the STM-1/OC3 CES modules, the VLAN interfaces TDMS2L and TDMS3L are set to be in the UP state permanently. These are the final states of the VLAN interfaces required for the STM-1/OC3 CES modules to operate properly.

[92] Initialization of the STM-1/OC3 CES modules starts when the hosting OS910-M is powered up.

# Configuration

## General

By default, the STM-1/OC3 CES module is set to operate with SDH. To set the STM-1/OC3 CES module to operate with SDH or SONET:

1. Enter **`enable`** mode
2. Invoke the command:
   **`tdm mode (sdh|sonet) slot (2|3)`**

> **Note**
> Execution of this command will erase the TDM configuration of the STM-1/OC3 CES module.

To view whether the STM-1/OC3 CES module in slot 2 or 3 is set to operate with SDH or SONET, refer to the section *Mode*, page *700*.

To configure an STM-1/OC3 CES module, first enter the TDM mode from **`configure terminal`** mode by invoking the following command:

**`tdm-oc3-stm1 SLOT-NUM`**

where,

**`SLOT-NUM`**: Number of the slot occupied by the STM-1/OC3 CES module. Valid numbers are 2 and 3.

Example

```
OS910-M# configure terminal
OS910-M(config)# tdm-oc3-stm1 2
OS910-M(config-tdm-oc3-stm1-2)#
```

## IP Address Assignment to an STM-1/OC3 CES Module

An IP address must be assigned to the STM-1/OC3 CES Module following clock settings. The IP address is required for operating in the CES protocols at Layer 2 and Layer 3.

To assign an IP address to the STM-1/OC3 CES Module, assign an IP address to a VLAN interface by invoking the command:

**`module-ip A.B.C.D/M interface vifN`**

where,

**`A.B.C.D/M`**: STM-1/OC3 CES module IP address with subnet prefix. This IP address should belong to a subnet configured on one of the OS910-M VLAN interfaces.

**`vifN`**: ID of existing VLAN interface having the format **`vifX`**, where **`X`** is a decimal number in the range **`1-4089`**. Example: **`vif3`**. The IP address of the interface must belong to the same subnet on which the STM-1/OC3 CES module resides. This VLAN interface will be permanently in the UP state.

Example

```
interface vlan vif10
 tag 10
 ip 1.1.1.1/8
 port 1

tdm 2
 clock mode internal
 module-ip 1.1.1.10/8 interface vif10
 session s1 description port_1
 session s1 port 1
 session s1 header-proto l3 target-ip 2.2.2.10
 session s1 local-udp-port 49152
 session s1 target-udp-port 49152
```

In the above example, an STM-1/OC3 CES module is in slot 2 (as indicated by the `2` in `tdm 2`). The IP address assigned to the STM-1/OC3 CES module is `1.1.1.10`, taken from the interface subnet of the VLAN interface `vif10`.

`vif10` will remain permanently UP independently of its member port 1, i.e., even if the port has no link, is unconnected, or connected to another device! Accordingly, `vif10` can be configured without any port as a member.

## Deleting IP Address Assigned to an STM-1/OC3 CES Module

To delete the IP address assigned to the STM-1/OC3 CES Module, invoke the command:

**`no module-ip`**

Example

```
OS910-M(config)# tdm 2
OS910-M(config-tdm2)# no module-ip
OS910-M(config-tdm2)#
```

## System Clock Source Selection

Select the system clock *source* by invoking the command:

**`clock system (internal|external|line)`**

where,

**`internal`**: On-board clock. (The clock is driven by a free-running internal oscillator - Stratum 3 OCXO.)

**`external`**: External clock. (The clock's frequency must one of the following: 8 KHz, 1.544 MHz, 2048 MHz, or 19.44 MHz. The on-board clock is locked to external clock's input.)

The external clock may be:

**`External-CLK-1`** (clock connected to CLK 1 RX port), or

**`External-CLK-2`** (clock connected to CLK 2 RX port),

**`line`**: SDH/SONET line. The on-board clock is locked to the received data stream at the STM-1/OC3 CES module interface P1 or P2.

## Service Clock Source Selection

The service (E1 or T1) clock is the clock of a single PDH circuit mapped to an E1/T1 channel of the STM-1/OC3 line.

The STM-1/OC3 CES module can provide a separate clock for each service (i.e., up to 63 clocks for the 63 E1 services and up to 84 clocks for the T1 services) or a common clock for all the services.

### All Services

To select a common service clock *source* for all the services (circuits or DS1[93] interfaces), invoke the command:

**`clock service mode (local|loopback)`**

where,

**`local`**: Source is system clock.

**`loopback`**: Source is the clock of a specific E1/T1 interface from the SDH/SONET line.

### Specific Services

To select a service clock *source* for specific services (circuits or DS1 interfaces), invoke the command:

**`clock service per-interface mode (local|loopback|recovery) IF`**

where,

**`local`**: Source is system clock.

**`loopback`**: Source is the clock of a specific E1/T1 interface from the SDH/SONET line.

[93] Digital Signal 1: A telecommunications-carrier signaling scheme devised by Bell Telephone Laboratories, Inc.

**recovery**: Source is a specific pseudowire on the Ethernet PSN. (Up 17 recovery service clocks can be assigned.)

**IF**: (a specific circuit). ID of a DS1 (E1/T1) interface is specified using the format:

**X1-1.K.L.M**

where,

**X1**: **E1** or **T1**

**K**: One of the three channels into which the carrier is divided.
It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided.
It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **1**, **2**, or **3**.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**

## External Clock Port-of-entry Selection

If an external clock is selected for the system clock, select its port of entry by invoking the command:

**clock input-ext source clk-in1 (smb1-rx|smb2-rx|other-slot|default) clk-in2 (smb1-rx|smb2-rx|other-slot|default)**

where,

**clk-in1**: External clock 1

**clk-in2**: External clock 2

**smb1-rx**: CLK 1 RX port (SMB connector)

**smb2-rx**: CLK 2 RX port (SMB connector)

**other-slot**: At CLK 1 RX port or Recovered (Ethernet PSN)

**default**: Default clock. The default may be **clk-in1** (smb1-rx) or **clk-in2** (smb2-rx).

## External Clock Frequency Specification

If an external source is selected for the system clock, specify its frequency by invoking the command:

**clock input-ext frequency (clk-in1|clk-in2) (1544|2048|8|19440|default)**

where,

**clk-in1**: External clock 1

**clk-in2**: External clock 2

**1544**: 1.544 MHz (for SONET)

**2048**: 2048 MHz (for SDH)

**8**: 8 KHz

**19440**: 19.44 MHz. (Default)

## External Clock for a Subsystem

### *Source* Selection

The output of the CLK 1 TX port or CLK 2 TX port of the STM-1/OC3 CES module can be used as an external clock to a subsystem.

To select the *source* of the external clock, invoke the command:

**clock output-ext source (ext|line|system)**

where,

`ext`: External clock 1 or 2

`line`: STM-1/OC3 line.

`system`: System clock

### Selection

To select an external clock for a subsystem, invoke the command:

**`clock output-ext fpanel smb1-tx from (clk-out1|other-slot|default) smb2-tx from (clk-out2|other-slot|default)`**

where,

`clk-out1`: Clock from CLK 1 TX port

`clk-out2`: Clock from CLK 2 TX port

`other-slot`: Clock-OUT-1 clock

`default`: Default clock. The default may be **`clk-out1`** (smb1-tx) or **`clk-out2`** (smb2-tx).

### Frequency Specification

To specify the frequency of an external clock for a subsystem, invoke the command:

**`clock output-ext frequency (8|ds1|19440|default)`**

where,

`19440`: 19.44 MHz

`8`: 8 KHz

`default`: Default (19.44 MHz)

`ds1`: DS1, i.e., 2.048 MHz for SDH mode of the STM-1/OC3 CES module, 1.544 MHz for SONET mode of the STM-1/OC3 CES module

### Admin Status Setting

To set the administrative status of an external clock for a subsystem, invoke the command:

**`clock output-ext admin-status (clk-out1|clk-out2) (enable|disable|default)`**

where,

`clk-out1`: Clock from CLK 1 TX port

`clk-out2`: Clock from CLK 2 TX port

`enable`: Enable external clock

`disable`: Disable external clock

`default`: Assign the default setting for external clock, i.e., enable.

## Automatic Protection Switching

Automatic Protection Switching (APS) for port-level redundancy enables switchover of a SONET/SDH circuit to a redundant circuit in the event of circuit failure.

This mechanism is supported on both the STM-1/OC3 CES module line interfaces P1 and P2.

### Enabling APS on both Interfaces

To enable APS on both interfaces P1 and P2, invoke the command:

**`aps`**

### Disabling APS on both Interfaces

To disable APS on both interfaces P1 and P2, invoke the command:

**`no aps`**

### Enabling only One Interface

To enable one interface and disable the other, invoke the command:

**`line (p1|p2)`**

where,

**p1**: STM-1/OC3 CES module interface P1

**p2**: STM-1/OC3 CES module interface P2

**Default**

To set the interfaces P1 and P2 in the default mode (P1 enabled, P2 disabled), invoke the command:

**default line**

## Transport Emulation Type

To specify the transport emulation type for the DS1 interface (E1/T1), invoke the CLI-command:

**interface <IF-STRING> transport-emulation-type (struct|unstruct)**

where,

**IF-STRING**: ID of a DS1 (E1/T1) interface is specified using the format:

**X1-1.K.L.M**

where,

**X1**: **E1** or **T1**

**K**: One of the three channels into which the carrier is divided.
It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided.
It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **1**, **2**, or **3**.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**

## Interface Admin State

To set administrative state of the interfaces, invoke the command:

**interface <IF-STRING> state (enable|disable)**

where,

**IF-STRING**: ID of interfaces: **stm1-1**, **stm1-2**, **oc3-1**, **oc3-2**, **sts-1.1**, **sts1-1.2**, **sts1-1.3**, or **X1-1.K.L.M**.

where,

**X1**: **E1**, **T1**, **VC12**, or **VT1.5**

**K**: One of the three channels into which the carrier is divided.
It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided.
It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **1**, **2**, or **3**.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**.

## Channel Bandwidth for Structured Mode

To define the *channel-bandwidth* for structured (framed) mode of the T1 DS1 interface, invoke the command:

**interface <IF-STRING> channel-bandwidth (64K|56K)**

**IF-STRING**: ID of DS1 interfaces: **X1-1.K.L.M**.

where,

**X1**: **T1**

**K**: One of the three channels into which the carrier is divided.
It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided.
It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the four channels into which the L channel is divided.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **t1-1.2.6.4**, **t1-1.3.7.4**.

## Frame Format for Structured Mode

To define the *frame format* for structured mode of the DS1 interface, invoke either of the following commands:

**interface <IF-STRING> frame-format (e1_pcm30|e1_pcm31|e1_pcm30crc|e1_pcm31crc)**

or

**interface <IF-STRING> frame-format (t1_esf|t1_d4)**

**IF-STRING**: ID of interfaces: **X1-1.K.L.M**.

where,

**X1**: **E1** or **T1**

**K**: One of the three channels into which the carrier is divided.
It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided.
It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **1**, **2**, or **3**.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**.

## Sessions

### Creating a New Session

To create a new session, invoke the command:

**session NAME description DESCR**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**DESCR**: Alphanumeric string of up to 31 characters.

To enable a session an interface must be assigned to it!

### Deleting a Session

To delete an existing session, invoke the command:

**no session NAME**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# no session s5
OS910-M(config-tdm-oc3-stm1-2)#
```

### E1/T1 Interface Assignment to a Session

Session activation on a specific E1/T1 interface depends on whether the interface is configured to structured or unstructured mode.

In unstructured mode all timeslots from the E1/T1 interface are assigned to one destination. The data stream from the interface, by definition, has no discernible time slots or other signaling information. The data stream is packetized according to the session header and other session parameters and then sent to the PSN.

In structured mode, all or a portion of the traffic from the interface can be sent to the target destination.

To assign an E1/T1 interface to a session in *structured mode with all timeslots* or in *unstructured* mode, invoke the command:

**`session NAME interface IF-STRING`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`IF-STRING`**: ID of interfaces: **`X1-1.K.L.M`**.

where,

**`X1`**: **`E1`** or **`T1`**

**`K`**: One of the three channels into which the carrier is divided.
It can have any of the values **`1`**, **`2`** or **`3`**.

**`L`**: One of the seven channels into which the K channel is divided.
It can have any of the values **`1`**, **`2`**, **`3`**, **`4`**, **`5`**, **`6`**, or **`7`**.

**`M`**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **`1`**, **`2`**, or **`3`**.
The four channels are T1.
A T1 channel can have any of the values **`1`**, **`2`**, **`3`**, or **`4`**.

Examples of valid formats are: **`e1-1.3.4.1`**, **`e1-1.2.5.3`**, **`t1-1.2.6.4`**, **`t1-1.3.7.4`**.

To assign an E1/T1 interface to a session in *structured mode with some timeslots*, invoke the command:

**`session NAME interface IF-STRING timeslots VALUE`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`IF-STRING`**: ID of interfaces: **`X1-1.K.L.M`**.

where,

**`X1`**: **`E1`** or **`T1`**

**`K`**: One of the three channels into which the carrier is divided.
It can have any of the values **`1`**, **`2`** or **`3`**.

**`L`**: One of the seven channels into which the K channel is divided.
It can have any of the values **`1`**, **`2`**, **`3`**, **`4`**, **`5`**, **`6`**, or **`7`**.

**`M`**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **`1`**, **`2`**, or **`3`**.
The four channels are T1.
A T1 channel can have any of the values **`1`**, **`2`**, **`3`**, or **`4`**.

Examples of valid formats are: **`e1-1.3.4.1`**, **`e1-1.2.5.3`**, **`t1-1.2.6.4`**, **`t1-1.3.7.4`**.

**`VALUE`**: Timeslots list.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s5 interface e1-1.1.1.1
OS910-M(config-tdm-oc3-stm1-2)#

OS910-M(config-tdm-oc3-stm1-2)# session s6 interface e1-1.1.1.2 timeslots 2-10
OS910-M(config-tdm-oc3-stm1-2)#
```

The session is enabled once a interface is assigned to it!

### Setting CES Protocol Header Format and Target Address

To set a SAToP or CESoPSN Header Format and a Target Address, invoke the command:

**`session NAME header-proto l3 target-ip A.B.C.D`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`l3`**: CES using Layer 3 SAToP or CESoPSN session header format.

**`A.B.C.D`**: Target IP address.

To set a CESoETH Header Format and a Target Address, invoke the command:

**`session NAME header-proto l2 target-mac MAC_ADDRESS`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`L2`**: CES using Layer 2 CESoETH session header format.

**`MAC_ADDRESS`**: Target MAC address in the format **`xx:xx:xx:xx:xx:xx`**, where **`x`** is a hexadecimal digit, e.g., **`8b:d0:e3:ac:28:f9`**.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s3 header-proto l2 target-mac 00:12:72:00:5e:4e
OS910-M(config-tdm-oc3-stm1-2)#

        or

OS910-M(config-tdm-oc3-stm1-2)# session s2 header-proto l3 target-ip 60.1.1.2
OS910-M(config-tdm-oc3-stm1-2)#
```

### Modifying the Description of an Existing Session

To modify the description of an existing session, invoke the command:

**`session NAME description DESCR`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`DESCR`**: Description. String upto 31 characters.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s5 description TEST-SESSiON-2
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting a Session's UDP Local Port

To set a session's UDP *local* port, invoke the command:

**`session NAME`** ***`local`*** **`-udp-port UDP-PORT`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`UDP-PORT`**: UDP local port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 local-udp-port 49152
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting a Session's UDP Target Port

To set a session's UDP *target* port, invoke the command:

**session NAME *target*-udp-port UDP-PORT**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**UDP-PORT**: UDP target port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 target-udp-port 49152
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting a Session's Out-of-stream (Signaling) UDP Local Port

To set a session's out-of-stream (signaling) UDP local port, invoke the command:

**session NAME local-oos-udp-port UDP-PORT**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**UDP-PORT**: UDP target port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 local-oos-udp-port 49152
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting a Session's Out-of-stream (Signaling) UDP Target Port

To set a session's out-of-stream (signaling) UDP target port, invoke the command:

**session NAME target-oos-udp-port UDP-PORT**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**UDP-PORT**: UDP target port number in the range 1 to 65535.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 target-oos-udp-port 49152
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the IP-ToS Field in the IP header of the CES Packet

The IP ToS field controls the priority of the CES traffic in an L3 session.

To set the IP ToS field, invoke the command:

**session NAME ip-tos (TOS)**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**TOS**: IP ToS value selectable from the range 0 to 255.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 ip-tos 184
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the *Local* Emulation Circuit ID for Unstructured Mode

To set the *local* Emulation Circuit ID (ECID) for a CESoETH Header in *unstructured* mode[94], invoke the command:

**session NAME local-ecid ECID**

where,

[94] Data and signaling are sent in the same session.

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 local-ecid 20
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the *Remote* Emulation Circuit ID for Unstructured Mode

To set the *remote* Emulation Circuit ID (ECID) for a CESoETH Header in *unstructured* mode, invoke the command:

**session NAME target-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 target-ecid 20
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the *Local* Emulation Circuit ID for Structured Mode

To set the *local* Emulation Circuit ID (ECID) for a CESoETH Header in *structured* mode[95], invoke the command:

**session NAME local-oos-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 local-oos-ecid 25
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the *Remote* Emulation Circuit ID for Structured Mode

To set the *remote* Emulation Circuit ID (ECID) for a CESoETH Header in *structured* mode, invoke the command:

**session NAME target-oos-ecid ECID**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**ECID**: Emulation Circuit ID selectable from the range 0 to 0xFFFFF.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 target-oos-ecid 25
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the Maximum Jitter Delay for a Session

To set the maximum jitter in milliseconds allowed for a session, invoke the command:

**session NAME jitter (MSEC)**

where,

**NAME**: ID of session in the format **s**NUM, where NUM is a number selectable from the range 1 to 100. Example: **s98**.

**MSEC**: Maximum jitter delay selectable from the range 1 to 64.

[95] For E1, in PCM-30 mode, data and signaling are sent in separate sessions.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 jitter 10
OS910-M(config-tdm-oc3-stm1-2)#
```

### Setting the Number of TDM Frames in Payload

To set the number of E1/T1 frames in the payload for a session, invoke the command:

**`session NAME payload-length (NUM)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`NUM`**: Number of TDM frames in payload.

For E1 the maximum allowed is 24.

For T1 the maximum allowed 32.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 payload-length 16
OS910-M(config-tdm-oc3-stm1-2)#
```

### Enabling/Disabling Payload Suppression

To enable or disable payload-suppression for a session, invoke the command:

**`session NAME payload-suppression (enable|disable|default)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`enable`**: Enable payload suppression.

**`disable`**: Disable payload suppression.

**`default`**: Disable payload suppression.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 payload-suppression enable
OS910-M(config-tdm-oc3-stm1-2)#
```

### Enabling/Disabling RTP Header Enable/Disable

To enable or disable RTP Header, invoke the command:

**`session NAME rtp-header (enable|disable|default)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`enable`**: Enable RTP header.

**`disable`**: Disable RTP header.

**`default`**: Disable RTP header.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 rtp-header enable
OS910-M(config-tdm-oc3-stm1-2)#
```

### Enabling or Disabling a Session

To enable or disable a session, invoke the command:

**`session NAME state (enable|disable)`**

where,

**`NAME`**: ID of session in the format **`s`**NUM, where NUM is a number selectable from the range 1 to 100. Example: **`s98`**.

**`enable`**: Enable state.

**`disable`**: Disable state.

Example

```
OS910-M(config-tdm-oc3-stm1-2)# session s2 state enable
OS910-M(config-tdm-oc3-stm1-2)#
```

#### Assigning a VLAN to a Session

To assign a VLAN with a VPT to a session, invoke the command:

**`session NAME vlan VLAN vpt VPT`**

where,

**`NAME`**: ID of session in the format **`sNUMBER`**, where NUM is a number selectable from the range 1 to 100. (Example: **`s98`**.)

**`VLAN`**: ID of VLAN (**`vif1`**, **`vif2`**, **`vif3`**, …, or **`vif4089`**).

**`VPT`**: VLAN priority tag (**`0`**, **`1`**, **`2`**, …, or **`7`**).

## Loopback

### Running

#### *Ethernet*

In this type of loopback, the test path extends from the STM-1/OC3 port (includes the P1 and P2 interfaces) over the Ethernet link and back.

To run Ethernet loopback, invoke the command:

**`interface stm1-1 loopback diagnostic`**

#### *Line*

In this type of loopback, the test path extends from the STM-1/OC3 port (includes the P1 and P2 interfaces) to the TDM and back.

To run Line loopback, invoke the command:

**`interface stm1-1 loopback line`**

### Stopping

To stop loopback, invoke the command:

**`interface stm1-1 loopback disable`**

## Link Reflection

The Link Reflection /Propagation or Link Integrity Notification (LIN) mechanism provides notification on the integrity of a link from the NNI (OS910-M data port) to the UNI (STM-1/OC3 port). It allows terminal equipment to detect link failure in the path between two terminal equipment units. The link failure is propagated throughout the network until it reaches the remote OS900, which disables the transmission immediately upon failure detection.

> **Note**
> If the uplink port is a trunk, then the trunk port is considered disabled if *all* ports of the trunk are disabled. Otherwise, it is considered enabled.

To enable Link Reflection:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`link-reflection-ces uplink PORT downlink (p1|p2) (direct|inverse) [symmetrical]`**

   where,

   **`PORT`**: Number of uplink Ethernet data port (possibly a trunk[96]). In the OS910-M model, the number must be between 1 and 10.

   **`p1`**: Physical Interface 1 for STM-1/OC3 – see *Figure 70*, page *680*.

[96] Described in detail in ***Chapter 13:*** *IEEE 802.3ad Link Aggregation (LACP)*, page *273*.

**p2**: Physical Interface 2 for STM-1/OC3 – see *Figure 70*, page *680*.

**direct**: Set the downlink port in the *same* state as the uplink port so that both ports are in enabled state or both are in disabled state.

**inverse**: Set the downlink port in the *opposite* state of the uplink port so that one port is in enabled state while the other is in disabled state.

**[symmetrical]**: *Without* the argument **symmetrical**, change in the *uplink port state* changes the downlink port state according to the argument **direct** and **inverse**, whichever was selected.
*With* the argument **symmetrical**, change in the *uplink* or *downlink port state* changes the downlink or uplink port state, respectively, according to the argument **direct** or **inverse**, whichever was selected.

## Alarms

### List

The list of all alarms about the STM-1/OC3 CES module that can be received is given below.

| *LEGEND* | |
|---|---|
| HH:MM:SS | Time of alarm (e.g., 14:46:53) |
| SLOT-NUM | Slot number (Left is 2, Right is 3) |
| CLOCK-NAME | Clock Name (e.g., C1, C2, ..., C8) |
| S-NAME | Session name (e.g., s1) |
| IF-NAME | Interface name (e.g., stm1-1, vc4-1, vc12-1.1.2.1, e1-1.1.1.1) |

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm RCV-FE-LOF.
*Denotation*: Far End sending Lost-Of-Frame.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm XMT-FE-LOF.
*Denotation*: Near End sending Lost-Of-Frame indication.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm RCV-AIS.
*Denotation*: Far End sending Alarm-Indication-Signal (AIS).

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm XMT-AIS.
*Denotation*: Near End sending AIS.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm LOF.
*Denotation*: Near End Lost-Of-Frame.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm LOS.
*Denotation*: Near End Lost-Of-Signal.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm LOOPBACK.
*Denotation*: Near End is Looped.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm RCV-TEST-CODE.
*Denotation*: Near End detects a test code.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm OTHER-FAILURE.
*Denotation*: Any line status not defined here.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm cleared.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm SectionNoDefect.
HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm SectionLOS.
*Denotation*: Near End Lost-Of-Signal.
(for section level: stm1-1/stm1-2)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm SectionLOF.

*Denotation*: Near End Lost-Of-Frame.
(for section level stm1-1/stm1-2)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm LineNoDefect.
HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm LineAIS.
*Denotation*: Near End sending AIS.
(for Line level: stm1-1/stm1-2)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm LineRDI.
*Denotation*: Remote Defect Indication is received from Far End.
(for Line level: stm1-1/stm1-2)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm PathNoDefect.
HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm PathSTSLOP.
*Denotation*: STS Path Loss of Pointer.
(for Path level: sts1-1.1)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm PathSTSAIS.
*Denotation*: STS Alarm-Indication-Signal.
(for Path level: sts1-1.1)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm PathSTSRDI.
*Denotation*: Remote Defect Indication.
(for Path level: sts1-1.1)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm PathUnequipped.
*Denotation*: Unequipped Signal.
(for Path level: sts1-1.1)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm PathSignalLabelMismatch.
*Denotation*: A Path connection is not correctly provosioned if a received Path label mismatch occurs.
(for Path level: sts1-1.1)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTNoDefect.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTLOP.
*Denotation*: VT Path Loss of Pointer.
(for VT level: vc12-1.1.1.1...vc12-1.3.7.3)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTPathAIS.
*Denotation*: VT Alarm-Indication-Signal.
(for VT level: vc12-1.1.1.1...vc12-1.3.7.3)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTPathRDI.
*Denotation*: Remote Defect Indication.
(for VT level: vc12-1.1.1.1...vc12-1.3.7.3)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTPathRFI.
*Denotation*: Remote Failure Indication.
(for VT level: vc12-1.1.1.1...vc12-1.3.7.3)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTUnequipped.
*Denotation*: Unequipped Signal. Remote Failure Indication.
(for VT level: vc12-1.1.1.1...vc12-1.3.7.3)

HH:MM:SS STM1 ALARM: slot SLOT-NUM, interface IF-NAME, msg: Alarm VTSignalLabelMismatch.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, clock CLOCK-NAME, msg: mode changed to Free Running.
HH:MM:SS STM1 ALARM: slot SLOT-NUM, clock CLOCK-NAME, msg: mode changed to Normal.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: jitter-buffer Underflow.

*Denotation*: No packets are present in the jitter buffer.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: jitter-buffer Overflow.
*Denotation*: Jitter buffer cannot accommodate newly arrived packets.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: jitter-buffer Normal.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: R-bit detect.
*Denotation*: Remote packet loss (on ETH) is indicated by reception of packets with their R bit set.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: excessive loss.
*Denotation*: Excessive packet loss rate is detected.

HH:MM:SS STM1 ALARM: slot SLOT-NUM, sessions S-NAME, msg: no defects.

### Indication

#### *Enabling*

To enable indication of alarms, invoke the command:

**`alarm`**

#### *Disabling*

To disable indication of alarms, invoke the command:

**`no alarm`**

### Target

To specify alarm target(s), invoke the command:

**`alarms target (all|cli|console|log|snmp)`**

where,

**`all`**: All targets
**`cli`**: CLI (TELNET/SSH) sessions
**`console`**: System console
**`log`**: System log
**`snmp`**: SNMP manager

To exlude alarm target to use the CLI-command:

**`no alarms target (all|cli|console|log|snmp)`**

where,

**`all`**: All targets
**`cli`**: CLI (TELNET/SSH) sessions
**`console`**: System console
**`log`**: System log
**`snmp`**: SNMP manager

## Routing

Invoke the commands specified in the section *Routing*, page *648*.

# Monitoring

## Mode

To view what mode (SDH or SONET) is set for the STM-1/OC3 CES module in slot 2 or 3 with which it is to operate:

1. Enter **`enable`** mode
2. Invoke the command:
   **`show tdm mode slot (2|3)`**

## APS Status

To view the APS configuration and statuses of the line interfaces P1 and P2, invoke the command:

**`show aps`**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show aps
Sonet/SDH APS State          :  Disable
Sonet/SDH Active Line        :  stm1-1 (0x10820000)
OS910M(config-tdm-oc3-stm1-2)#
```

## Clock Configurations

### All

To view the system and all service clock configurations, invoke the command:

**`show clock config all`**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show clock config all
System     : line
Interface  : Clock Mode
-----------: --------------------
e1-1.1.1.1 : loopback
e1-1.1.1.2 : loopback
e1-1.1.1.3 : loopback
e1-1.1.2.1 : loopback
e1-1.1.2.2 : loopback
e1-1.1.2.3 : loopback
e1-1.1.3.1 : loopback
e1-1.1.3.2 : loopback
e1-1.1.3.3 : loopback
e1-1.1.4.1 : loopback
e1-1.1.4.2 : loopback
e1-1.1.4.3 : loopback
e1-1.1.5.1 : loopback
e1-1.1.5.2 : loopback
e1-1.1.5.3 : loopback
e1-1.1.6.1 : loopback
.....................
.....................
e1-1.3.7.1 : loopback
e1-1.3.7.2 : loopback
e1-1.3.7.3 : loopback
OS910M(config-tdm-oc3-stm1-2)#
```

### Specific

To view the system and specific service clock configurations for a DS1 interface, invoke the command:

**`show clock config interface < INTERFACE>`**

where,

**< INTERFACE>**: **system|IF-STRING**

**system**: System interface

**IF-STRING**: ID of interfaces: **X1-1.K.L.M**.

where,

**X1**: **E1** or **T1**

**K**: One of the three channels into which the carrier is divided. It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided. It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **1**, **2**, or **3**.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**

Example 1

```
OS910M(config-tdm-oc3-stm1-2)# show clock config interface system

   Clock Configuration
--------------------------------
System Mode         : line
Service clock       : loopback
OS910M(config-tdm-oc3-stm1-2)#
```

Example 2

```
OS910M(config-tdm-oc3-stm1-2)# show clock config interface e1-1.1.1.2

   Clock Configuration
--------------------------------
System Mode         : line
Service clock       : loopback
OS910M(config-tdm-oc3-stm1-2)#
```

## Clock Status

To view the system and service clock status, invoke the command:

**show clock status interface <IF-NAME>**

where,

**<IF-NAME>**: **system1|system2|DS1-interface**

**system1**: System 1

**system2**: System 2

**DS1-INTERFACE** : ID of interfaces: **X1-1.K.L.M**.

where,

**X1**: E1 or T1

**K**: One of the three channels into which the carrier is divided. It can have any of the values **1**, **2** or **3**.

**L**: One of the seven channels into which the K channel is divided. It can have any of the values **1**, **2**, **3**, **4**, **5**, **6**, or **7**.

**M**: One of the three/four channels into which the L channel is divided.
The three channels are E1.
An E1 channel can have any of the values **1**, **2**, or **3**.
The four channels are T1.
A T1 channel can have any of the values **1**, **2**, **3**, or **4**.

Examples of valid formats are: **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**

Example 1

```
OS910M(config-tdm-oc3-stm1-2)# show clock status interface system1
Input state                   :  Active
Clock mode                    :  Free running
Recovery method               :  Direct
Input status                  :  Not locked
Priority                      :  0
Lbit failure                  :  Enable
Packet missorder failure      :  Disable
Recovery degraded failure     :  Disable
Source interface              :  0x10820000
Clock index                   :  99
OS910M(config-tdm-oc3-stm1-2)#
```

Example 2

```
OS910M(config-tdm-oc3-stm1-2)# show clock status interface e1-1.2.1.2
Input state                   :  Active
Clock mode                    :  Normal
Recovery method               :  Direct
Input status                  :  Locked
Priority                      :  0
Lbit failure                  :  Enable
Packet missorder failure      :  Disable
Recovery degraded failure     :  Disable
Source interface              :  0x10834540
Clock index                   :  29
OS910M(config-tdm-oc3-stm1-2)#
```

## External Clock for a Subsystem

To view the what external clocks are selected for subsystem(s), invoke the command:

**show external-clock**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show external-clock
HW shadow value               : 0x60
External clk-in1 get from     : SMB-1-Rx
External clk-in2 get from     : SMB-2-Rx
SMB-1-Tx get from             : clk-out1
SMB-2-Tx get from             : clk-out2
Backplane get from            : clk-out1
----------  External Clock In #1 ----------
Frequency                     : 19440K
If Index                      : 0x3c008000
RTP timestamp rate            : 5
Direction                     : Input
----------  External Clock In #2 ----------
Frequency                     : 19440K
If Index                      : 0x3c010000
RTP timestamp rate            : 5
Direction                     : Input
----------  External Clock Out ----------
If Index 1                    : 0x3c808000
Ext Out 1 admin status        : Enable
If Index 2                    : 0x3c810000
Ext Out 2 admin status        : Enable
Clock Speed                   : 19440K
Source Clock                  : System-Clock
Source If                     : None
OS910M(config-tdm-oc3-stm1-2)#
```

## Interface Status

To view the administrative and operation status of the STM-1/OC3 CES module or interface, invoke the command:

**show interface config <IF-NAME>**

Example 1

```
OS910M(config-tdm-oc3-stm1-2)# show interface config stm1-1
Admin Status                 :  Down
Loopback config              :  NoLoop
OS910M(config-tdm-oc3-stm1-2)#
```

Example 2

```
OS910M(config-tdm-oc3-stm1-2)# show interface config vc12-1.1.1.1
Admin Status                 :  Up
OS910M(config-tdm-oc3-stm1-2)#
```

Example 3

```
OS910M(config-tdm-oc3-stm1-2)# show interface config e1-1.1.1.1
Admin Status                 :  Up
Line format                  :  E1
Framed mode                  :  Unframed
Frame format                 :  -
Channel bandwidth            :  -
OS910M(config-tdm-oc3-stm1-2)#
```

## Alarms

### Indication

To view whether alarm indication is enabled or disabled, invoke the command:

**show alarms configuration**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show alarms configuration

   Alarms reporting is Enable.
OS910M(config-tdm-oc3-stm1-2)#
```

### Targets

To view the alarm target(s), invoke the command:

**show alarms target**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show alarms target
 alarms target cli
 alarms target log
OS910M(config-tdm-oc3-stm1-2)#
```

### Status of Interface

To view the alarm status of the interfaces of an STM-1/OC3 CES module, invoke the command:

**show interface alarms (ds1|line|path|section|vt) (<IF-NAME>|all)**

where,

**ds1**: DS1 level interface (e.g., **e1-1.3.4.1**, **e1-1.2.5.3**, **t1-1.2.6.4**, **t1-1.3.7.4**)

**line**: Line level interface (**stm1-1**, **stm1-2**, **oc3-1**, or **oc3-2**)

**path**: Path level interface (**vc4-1**, **vc4-2**, **sts-1.1**, **sts1-1.2**, or **sts1-1.3**)

**section**: Section level (**stm1-1**, **stm1-2**, **oc3-1**, or **oc3-2**)

**vt**: VT level (e.g., **vc12-1.3.4.1**, **vt1.5-1.2.6.4**)

Example 1

```
OS910M(config-tdm-oc3-stm1-2)# show interface alarms ds1 e1-1.1.1.1
Line status                  :  RcvAISXmtAIS
OS910M(config-tdm-oc3-stm1-2)#
```

Example 2

```
OS910M(config-tdm-oc3-stm1-2)# show interface alarms section stm1-1
Current Status                          :  Unknown
Num of Errored Seconds (ES)             :  0
Num of Severely Errored Seconds (SES)   :  0
Num of Severely Err Framed Secs (SEFS)  :  0
Num of Coding Violations (CV)           :  0
OS910M(config-tdm-oc3-stm1-2)#
```

Example 3

```
OS910M(config-tdm-oc3-stm1-2)# show interface alarms path vc4-1
Width                                   :  1(sts1)
Current Status                          :  4(STSAIS)
Num of Errored Seconds (ES)             :  0
Num of Severely Errored Seconds (SES)   :  0
Num of Coding Violations (CV)           :  0
Num of Unavailable Seconds (UAS)        :  445
OS910M(config-tdm-oc3-stm1-2)#
```

## Sessions

### Operation Status

#### *Brief*

To view the operation status of sessions in brief, invoke the command:

**show session**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show session

Name Description                      modified_config    running_config
-------------------------------------------------------------------------
s1   a                                Session Enabled    Session running
s2   b                                Session Enabled    Session running
s3   c                                Session Enabled    Session running
s4   d                                Session Enabled    Session running
s5   SSSS5                            Session Enabled    Session running
OS910M(config-tdm-oc3-stm1-2)#
```

#### *Detail*

To view the operation status of sessions in detail, invoke the command:

**show session detail**

Example

```
OS910M(config-tdm-oc3-stm1-2)# show session detail


--------------------------------------------------------------------------------
 Sess |Tdm-If     |Loc Udp |Target IP         |Targ UDP|TDM frame |VLAN |State
 Abbr |           |/ECID   |/MAC              |/ECID   |Mode      |/MPLS|
--------------------------------------------------------------------------------
s1    |e1-1.1.1.1 |100     |00:12:72:00:63:8e |100     |Unframed  |VLAN |En
s2    |e1-1.1.1.2 |200     |00:12:72:00:63:8e |200     |Unframed  |VLAN |En
s3    |e1-1.1.1.3 |300     |00:12:72:00:63:8e |300     |Unframed  |VLAN |En
s4    |e1-1.1.2.1 |400     |00:12:72:00:63:8e |400     |Unframed  |VLAN |En
s5    |e1-1.2.1.2 |42      |00:11:22:11:22:11 |42      |Unframed  |VLAN |En
--------------------------------------------------------------------------------
OS910M(config-tdm-oc3-stm1-2)#
```

### Configuration Status

To view the configuration of a session, invoke the command:

**show session detail <SESSION> config**

<u>Example</u>

```
OS910M(config-tdm-oc3-stm1-2)# show session detail s1 config

                CONFIGURATION

Item                          :  Value
------------------------------:  ---------
Session mode                  :  Enable
Header type                   :  CESoETH
Local ECID                    :  100
Target ECID                   :  100
Target MAC                    :  00:12:72:00:63:8e
Payload length (frames)       :  8
Jitter maximum level (ms)     :  5
VLAN enable                   :  Enable
VLAN-ID                       :  100
VLAN priority (VPT)           :  6
MPLS enable                   :  Disable
RTP  enable                   :  Disable
Transport emulation type      :  Unstructured
Session bandwidth (in Kbps)   :  2288
Payload suppresion            :  Disable
TDM interface                 :  e1-1.1.1.1
Time Slots                    :  1-32
OS910M(config-tdm-oc3-stm1-2)#
```

### Diagnostic Status

To view the diagnostic status of a session, invoke the command:

**show session detail <SESSION> status**

<u>Example</u>

```
OS910M(config-tdm-oc3-stm1-2)# show session detail s1 status

                STATUS/STATISTICS

Item                               :  Status/Value
-----------------------------------:  ---------
Eth to TDM direction               :  DOWN
TDM to Eth direction               :  DOWN
PSN Rx status                      :  LOPS
PSN Tx status                      :  UP + R-bit Tx On
Current jitter buffer delay (ms)   :  -
Jitter maximum level (ms)          :  -
Jitter minimum level (ms)          :  -
Valid Eth packets per sec          :  0
Handled Eth packets                :  0
Late Eth packets                   :  0
Lost Eth packets                   :  0
Packets per seconds                :  1000
Packets with L-bit                 :  0
Packets with R-bit                 :  0
Underrun Eth packets               :  8951391
Overrun Eth packets                :  0
Malformed packets counter          :  0
Duplicate Eth packets              :  0
Missing Eth packets                :  0
OS910M(config-tdm-oc3-stm1-2)#
```

### Diagnostic Status

To view the configuration and diagnostic status of a session, invoke the command:

**`show session detail <SESSION>`**

<u>Example</u>

```
OS910M(config-tdm-oc3-stm1-2)# show session detail s1

                CONFIGURATION

Item                          :  Value
------------------------------:  ---------
Session mode                  :  Enable
Header type                   :  CESoETH
Local ECID                    :  100
Target ECID                   :  100
Target MAC                    :  00:12:72:00:63:8e
Payload length (frames)       :  8
Jitter maximum level (ms)     :  5
VLAN enable                   :  Enable
VLAN-ID                       :  100
VLAN priority (VPT)           :  6
MPLS enable                   :  Disable
RTP  enable                   :  Disable
Transport emulation type      :  Unstructured
Session bandwidth (in Kbps)   :  2288
Payload suppresion            :  Disable
TDM interface                 :  e1-1.1.1.1
Time Slots                    :  1-32

                STATUS/STATISTICS

Item                               :  Status/Value
-----------------------------------:  ---------
Eth to TDM direction               :  DOWN
TDM to Eth direction               :  DOWN
PSN Rx status                      :  LOPS
PSN Tx status                      :  UP + R-bit Tx On
Current jitter buffer delay (ms)   :  -
Jitter maximum level (ms)          :  -
Jitter minimum level (ms)          :  -
Valid Eth packets per sec          :  0
Handled Eth packets                :  0
Late Eth packets                   :  0
Lost Eth packets                   :  0
Packets per seconds                :  1000
Packets with L-bit                 :  0
Packets with R-bit                 :  0
Underrun Eth packets               :  9056391
Overrun Eth packets                :  0
Malformed packets counter          :  0
Duplicate Eth packets              :  0
Missing Eth packets                :  0
OS910M(config-tdm-oc3-stm1-2)#
```

# Product Specification

| | |
|---|---|
| Purpose | Connection to STM-1 or OC3 line. |
| TDM Traffic | Fractional (DS0 granularity) full structured & unstructured mode of pseudowire formation. |
| Emulated Circuits | Up to 63 E1 services or 84 T1 services. |
| Circuit Emulation Protocols | SAToP, CESoPSN, CESoETH MEF-8 |
| Data Rate (STM-1 or OC3 line) | Up to 155.52 Mbps (payload: 148.608 Mbit/s; overhead: 6.912 Mbps, including path overhead) over fiberoptic networks using Telcordia Technologies GR-253-CORE.GR |
| Standards | ANSI, T1.105-1995, T1.105.02, T1.231-1997<br>AT&T-TR 54016, TR 62411<br>Bell Communications Research TA-TSY-000191, TRNWT-000233, TR-TSY-000303<br>ETS - IETS 300 417-1-1, January 1996<br>ITU-T G.707, G.781, G.783, G.783 Amendment 1, June 2002 |
| Clocking | Adaptive, Internal, External, Loopback, Line<br>Jitter/Wander Compliance G.823/G.824<br>Configure Jitter compensation 0.25 ms to 256 ms<br>Synchronization over packet based on IEEE1588v2 |
| Cabling | Per the SFP |
| Power Consumption (Max) | 17 W |

# Chapter 40: DSL Setup and Monitoring

## General

The OS904-DSL4 can concurrently function also as a Single-pair High-speed Digital Subscriber Line (SHDSL) transceiver. It has four Ethernet ports and one DSL port. The number IDs of the Ethernet ports are 1 to 4. The number ID of the DSL port is 5. The DSL port has 4 DSL channels.

‘Set’ commands for configuring the DSL port and its channels are found in **`dsl 5`** mode.

'Show' commands for DSL are found in **`enable`** mode.

## Set CLI Commands

### Accessing Set Commands

To access set commands for configuring the DSL port and its channels enter **`dsl 5`** mode by invoking the following sequence of commands:

**`enable`** → **`configure terminal`** → **`dsl 5`**

### DSL PORT

#### Enabling/Disabling

To enable the DSL port, invoke the command:

**`enable`**

To disable the DSL port (Default state), invoke the command:

**`no enable`**

#### CO/CPE

To set the DSL port to operate as a CO[97] (STU-C) or CPE[98] (STU-R) invoke the command:

**`mode co|cpe`**

Where,

**`co`**: CO state.

**`cpe`**: CPE state. (Default.)

Note: The DSL line must connect a DSL port set as CPE to a DSL port set as CO.

### DSL CHANNEL

#### Flow Type

To specify flow type for all the channels of the port, invoke the command:

**`flow efm|atm`**

where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`efm`**: Ethernet (in the first mile). (This is the default state.)

**`atm`**: Asynchronous Transfer Mode

To set the flow type to the default (**`efm`**), invoke the command **`no flow`**

[97] Central Office

[98] Customer Premises Equipment

### PAF Fragmentation Size

To specify fragments size when working at flow EFM, invoke the command:

**`paf-frag-size <64-512>`**

Where,

`<64-512>`: Range of sizes in bytes. The size must be a multiple of 4 bytes.

To set the fragment size to the default (**256 bytes**), invoke the command **no paf-`frag-size`**.

### Operation State

To set the operation state for the channels of the port, invoke the command:

**`channel CHANNELS oper-state enable|disable|restart`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`enable`**: Enable channels. (Default)

**`disable`**: Disable channels.

**`restart`**: Restart (disable followed by enable) channels.

To set the channel state to the default (**`enable`**), invoke the command **`no channel CHANNELS oper-state`**

### Loop-Attenuation-Alarm Threshold

To set the loop-attenuation-alarm threshold, invoke the command:

**`channel CHANNELS eoc-thresh-loop-att <0-127>`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

`<0-127>`: Loop-attenuation-alarm threshold. The range is `<0-127>` in dB. (Default: `0`, i.e., no alarm)

To set the loop-attenuation-alarm threshold to the default (no alarm), invoke the command:

**`no channel CHANNELS eoc-thresh-loop-att`**

### SNR-Margin-Alarm Threshold

To set the SNR-margin-alarm threshold, invoke the command:

**`channel CHANNELS eoc-thresh-snr-marg <0-15>`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

`<0-15>`: SNR-margin-alarm threshold. The range is `<0-15>` in dB. (Default: `0`, i.e., no alarm)

To set the SNR-margin-alarm threshold to the default (no alarm), invoke the command:

**`no channel CHANNELS eoc-thresh-snr-marg`**

### Enabling/Disabling Remote (STU-R) EOC Management

To enable (default) remote (STU-R) EOC Management, invoke the command:

**`channel CHANNELS eoc-management enable`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

To disable remote (STU-R) EOC Management, invoke the command:

**`no channel CHANNELS eoc-management`**

### Downstream/Upstream Current-Condition Target SNR Margin

To set the downstream/upstream current-condition target SNR margin, invoke the command:

**`channel CHANNELS pmms-snr-curr-marg VALUE`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`VALUE`**: Downstream/upstream current-condition target SNR margin. The range is `<-10-21>` in dB. (Default: `0`, i.e., no margin)

To set the downstream/upstream current-condition target SNR margin to the default (no margin), invoke the command:

**`no channel CHANNELS pmms-snr-curr-marg VALUE`**

### Downstream/Upstream Worst-Case Target SNR Margin

To set the downstream/upstream worst-case target SNR margin, invoke the command:

**`channel CHANNELS pmms-snr-worst-marg VALUE`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`VALUE`**: Downstream/upstream worst-case target SNR margin. The range is **`<-10-21>`** in dB. (Default: **`0`**, i.e., no margin)

To set the downstream/upstream worst-case target SNR margin to the default (no margin), invoke the command:

**`no channel CHANNELS pmms-snr-worst-marg`**

### Enabling Line Rate

To allow (default) the line rate set *automatically by DSL port* to be used, invoke the command:

**`channel CHANNELS pmms-state enable`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

To allow the line rate set *manually by the user* to be used, invoke the command:

**`no channel CHANNELS pmms-state`**

### PAM Constellation Selection

To select the PAM constellation, invoke the command:

**`channel CHANNELS tc-pam pam16|pam32|auto`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`pam16`**: PAM_16 constellation option requiring that the data rate be limited to a value between 192 kbps and 3840 kbps

**`pam32`**: PAM_32 constellation option requiring that the data rate be limited to a value between 768 kbps and 5696 kbps

**`auto`**: Automatic selection of the PAM by the OS904-DSL4. (Default)

To set the PAM constellation option to the default (**`auto`**), invoke the command:

**`no channel CHANNELS tc-pam`**

### Capability List Style Selection

By default, the new capability list supports code points for EFM and extended data rates.
The old capability list (according to G.shdsl, i.e, old SHDSL standard) supports code points up to 2312 kbps only.

Note: The options **`auto`** and **`old`** of the capability list must only be applied on a CPE (STU-R) when the flow type is **`atm`** – see section *Flow Type*, page *709*. The options **`auto`** and **`old`** cannot be applied for EFM flow.

To select the capability list style, invoke the command:

**`channel CHANNELS cap-list-style new|old|auto`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`new`**: New capability list standard. (Default)

**`old`**: Old capability list standard.

**`auto`**: Automatic selection of capability list standard.

To set the capability list style to the default (**`new`**), invoke the command:

**`no channel CHANNELS cap-list-style`**

### SHDSL Line Wire Mode

This option applies only for the flow type **atm** – see section *Flow Type*, page *709*.

To select the SHDSL line wire mode, invoke the command:

**channel CHANNELS wiring 2-wire|4-wire**

Where,

**CHANNELS**: One or more channel IDs selectable from the range 1 to 4.

**2-wire**: 2-wire mode. (Default)

**4-wire**: 4-wire mode. Also called "enhanced mode" (GSPN). Applicable only for STU-R

To set the SHDSL line wire mode to the default (**2-wire**), invoke the command:

**no channel CHANNELS wiring**

### Setting Line Rate

The line rate is either the maximum rate for auto mode or according to the manually selected line rate for manual mode. Its mode setting is described in section *Enabling Line* Rate, page *711*.

Constraint: The highest line rate assigned to a channel can be at most four times as large as the lowest line rate assigned to any other channel.

To set the line rate, invoke the command:

**channel CHANNELS line-rate <192000-5696000>**

Where,

**CHANNELS**: One or more channel IDs selectable from the range 1 to 4.

**<192000-5696000>**: Range of line rates in bps with 64000 bps granulation. (Default: **5696000**)

To set the line rate to the default (**5696000**), invoke the command:

**no channel CHANNELS line-rate [<192000-5696000>]**

### SHDSL Transmission Mode

Either of the two transmission modes[99] (regional settings) Annex A/F (US) and Annex B/G (European) can be selected. To specify the transmission mode for the SHDSL line, invoke the command:

**channel CHANNELS annex annex-a/f|annex-b/g**

Where,

**CHANNELS**: One or more channel IDs selectable from the range 1 to 4.

**annex-a/f**: US standard.

**annex-b/g**: European standard. (Default)

To set the transmission mode to the default (**annex-b/g**), invoke the command:

**no channel CHANNELS annex**

### Reference Clock

To specify the reference clock for a DSL link, invoke the command:

**channel CHANNELS clk-mode clk-1|clk-2|clk-3a|clk-3b**

Where,

**CHANNELS**: One or more channel IDs selectable from the range 1 to 4.

**clk-1**: Plesiochronous

**clk-2**: Plesiochronous with timing reference

**clk-3a**: Synchronous. (Default)

**clk-3b**: Hybrid: downstream: synchronous upstream: plesiochronous

To select the default reference clock (**clk-3a**), invoke the command:

**no channel CHANNELS clk-mode**

---

99 Annex A and B are old standards and specify the rate 2.3 Mbps as maximum. Annex F and G are new standards and extend the maximum rate to 5.7 Mbps.

### Clock Direction

To specify the clock direction for a DSL link, invoke the command:

**`channel CHANNELS clk-dir default|input|output`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`default`**: CO is input and CPE is output.

**`input`**: Clock direction from remote source

**`output`**: Clock direction from local source

To select the default clock direction (**`default`**), invoke the command:

**`no channel CHANNELS clk-dir`**

### Power Backoff Mode

To set the power backoff mode, invoke the command:

**`channel CHANNELS pbo-mode force|normal`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`force|normal`**: Force power.

**`normal`**: Automatic detection.

To set the power backoff mode to the default (**`normal`**), invoke the command:

**`no channel CHANNELS pbo-mode`**

### Power Backoff Setting

This option is used to reduce the power *attenuation* (possibly due to cross-talk) in a bundle of channels.

To set the power backoff value, invoke the command:

**`channel CHANNELS pbo-value <1-31>`**

Where,

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`<1-31>`**: Range of power backoff values in dB. (Default: **`0`**, i.e., no backoff)

To set the power backoff mode to the default (**`0`**), invoke the command:

**`no channel CHANNELS pbo-value`**

### Estimated Power Loss Mode

To enable/disable calculation of the EPL for PBO, invoke the command:

**`channel CHANNELS pbo-epl enable|disable`**

**`CHANNELS`**: One or more channel IDs selectable from the range 1 to 4.

**`enable`**: Enable calculation. (Default)

**`disable`**: Disable calculation.

To set the calculation mode to the default (**`enable`**), invoke the command:

**`no channel CHANNELS pbo-epl`**

## Viewing Running Configuration

### Port

To view run-time configuration information on the DSL port, invoke the command:

**`show running-config dsl [5]`**

Example 1

The example shows the OS904-DSL4 is configured as a CO.

```
dsl 5
   mode co
   enable
```

Example 2

The example shows the OS904-DSL4 is configured as a CPE.

```
dsl 5
   enable
```

**Channels**

To view run-time configuration information on the DSL port's channels, invoke the command:

**`show running-config dsl 5 channel <1-4>`**

Where,

**`<1-4>`**: One or more channel IDs selectable from the range 1 to 4.

# Viewing General Port Information

To view information about all ports of the OS904-DSL4, invoke the command:

**`show port`**

Example

```
PORT   MEDIA     MODE_SELECT  LINK  SPEED_SEL   LAN_SPD   DUPL STATE     SL
--------------------------------------------------------------------------
1      TP        COPPER       OFF  AUTO         N/A         N/A  ENABLE  1
t1     ---       ---          OFF  AUTO         N/A         N/A  ENABLE  1
(2)    TP        COPPER       OFF  AUTO         N/A         N/A  ENABLE  1
(3)    TP        COPPER       OFF  AUTO         N/A         N/A  ENABLE  1
4      TP        COPPER       OFF  --           N/A         N/A  ENABLE  1
5      DSL       COPPER       ON   --           --           --  ENABLE  1
(5.0)  --        --           ON   --           N/A         N/A  ENABLE  -
(5.1)  --        --           ON   --           N/A         N/A  ENABLE  -
(5.2)  --        --           ON   --           N/A         N/A  ENABLE  -
(5.3)  --        --           ON   --           N/A         N/A  ENABLE  -
```

# Viewing SHDSL Configuration

To view DSL port and channel configuration, invoke the command:

**`show dsl 5 channel <1-4>`**

Where,

**`<1-4>`**: One or more channel IDs selectable from the range 1 to 4.

Example

```
DSL port #5 Mode: CO, Flow:EFM

Aggregation is UP

Aggregation Fragment size is 256 bytes

----------------------------------------

DSL Channel #1

Parameter                      AdminState          OperState

--------------------------------------------------------------

DSL Process                                        Data

Aggregated                                         Yes

PSD Mask                       Symmetric

Wiring                         Two

Port State                     Enable              Up

Line Probe State               Enable

Probe SNR current margin (dB)  0

Probe SNR worst margin (dB)    0

TC-PAM                         auto                pam32

Line Rate (bps)                5696000             5696000

EOC Management                 Enable              Enable

EOC loop attenuation (dB)      0(threshold)        0

EOC SNR margin (dB)            0(threshold)        20

PBO Mode                       normal

PBO Value (dB)                 0                   6

PBO EPL                        Enable

Annex                          Annex B/G           Annex B/G

Capabilities List Style        new                 new

Clock Mode                     3a (Synchronous)

Clock Direction                default             input

------------------------
DSL port #5 is enabled
```

# Viewing SHDSL Statistics

## For Line Side

To view statistical information on the DSL port’s line side, invoke the command:

**`show dsl-counters-line-side 5`**

Example

```
DSL Port#5

Counter Name                                                Counter Value

---------------------------------------------------------------------------

Frames Transmitted OK                                       399602

Frames Received OK                                          399603

Frame Check Sequence Errors                                 1

Alignment Errors                                            1

Octets Transmitted OK                                       99901

Octets Received OK                                          99900

Frames Lost Due To Internal MAC sublayer Transmit Error     1

Frames Lost Due To Internal MAC sublayer Receive Error      2

PAUSE frames passed to MAC sublayer for transmission        1

PAUSE frames passed by MAC sublayer to MAC control sublayer  2

Frame Too Long Errors                                       3

Frame Too Short Errors                                      5
```

## For Channels

To view statistical information on the DSL port's channels, invoke the command:

**show dsl-counters 5 channel <1-4>**

Where,

**<1-4>**: One or more channel IDs selectable from the range 1 to 4.

Example

```
Counter Name                             Counter Value

----------------------------------------------------

Code Violation Error Counter             0

Erroneous Seconds Counter                0

Severely Erroneous Seconds Counter       0

LOSWS Counter                            1

Unavailable Seconds Counter              0

Elapsed Time                             450
```

# Clearing SHDSL Statistics

## For Line-Side

To clear SHDSL line-side statistical counters of the DSL port, invoke the command:

**`clear dsl-counters-line-side 5`**

## For Channel

To clear SHDSL channel statistics, invoke the command:

**`clear dsl-counters 5 channel <1-4>`**

Where,

**`<1-4>`**: One or more channel IDs selectable from the range 1 to 4.

The command **`clear dsl-counters 5`** will clear both line-side and channel counters.

# Chapter 41: MultiProtocol Label Switching (MPLS)

## General

MPLS is a technology that uses labels to direct traffic (e.g., Ethernet packets) to their destination. With MPLS it is possible to overcome the following major *drawbacks* of conventional routing:

- No support for traffic engineering because IP networks are connectionless.
- Difficulty in implementing complex QoS architectures.

While overcoming the abovementioned drawbacks, MPLS has the following additional advantages:

- Scalable solution - Labels are local and several IP addresses can be associated with one or more labels.
- Simple solution - The interior Label Switch Routers (LSRs) perform simple label switching. Only the Label Edge Routers (LERs) perform the more complicated task of classifying the packets into FEC[100] and binding a label.
- Lower latency - Usually label-switching is a simple task compared with the longest prefix match and IP forwarding. The amount of per-packet processing is reduced.
- More importantly, provides capabilities of connection-oriented technologies, notably ATM, that include:
  - Traffic engineering (optimization of network utilization, dynamic definition of routes, resource allocation according to demand and availability)
  - QoS
  - VPNs

An MPLS domain is built of LERs (Label Edge Routers) that reside at the edge of MPLS domain and interior LSRs (Label Switch Routers) that are located within the MPLS domain – see *Figure 71*. The LERs need to deal with both MPLS frames and native protocol traffic while Interior LSRs need to forward only MPLS frames.

Following are the main functions performed on a flow in an MPLS network:

1. The Ingress Label Edge Router (LER) examines each inbound packet, classifies the packet according to a Forwarding Equivalence Class (FEC), generates an MPLS header, and assigns (binds) an initial label.
2. All the other routers inside the MPLS domain (interior LSRs) examine only the MPLS labels in order to make forwarding decisions while performing label switching.
3. The Egress LER removes the label and forwards the packet based on the native protocol address.

**Note**

The OS900 can function as an LER and not as an LSR. The OS9000 can function as an LER or LSR. Accordingly, a complete MPLS network can be built with OS900s as LERs and OS9000s as LSRs.

[100] FEC (Forwarding Equivalence Class) is a group of IP packets which are forwarded in the same manner and over the same path. A FEC may be associated with any class of traffic that the LER considers significant. An example of a FEC is all traffic having a specific value of IP precedence.

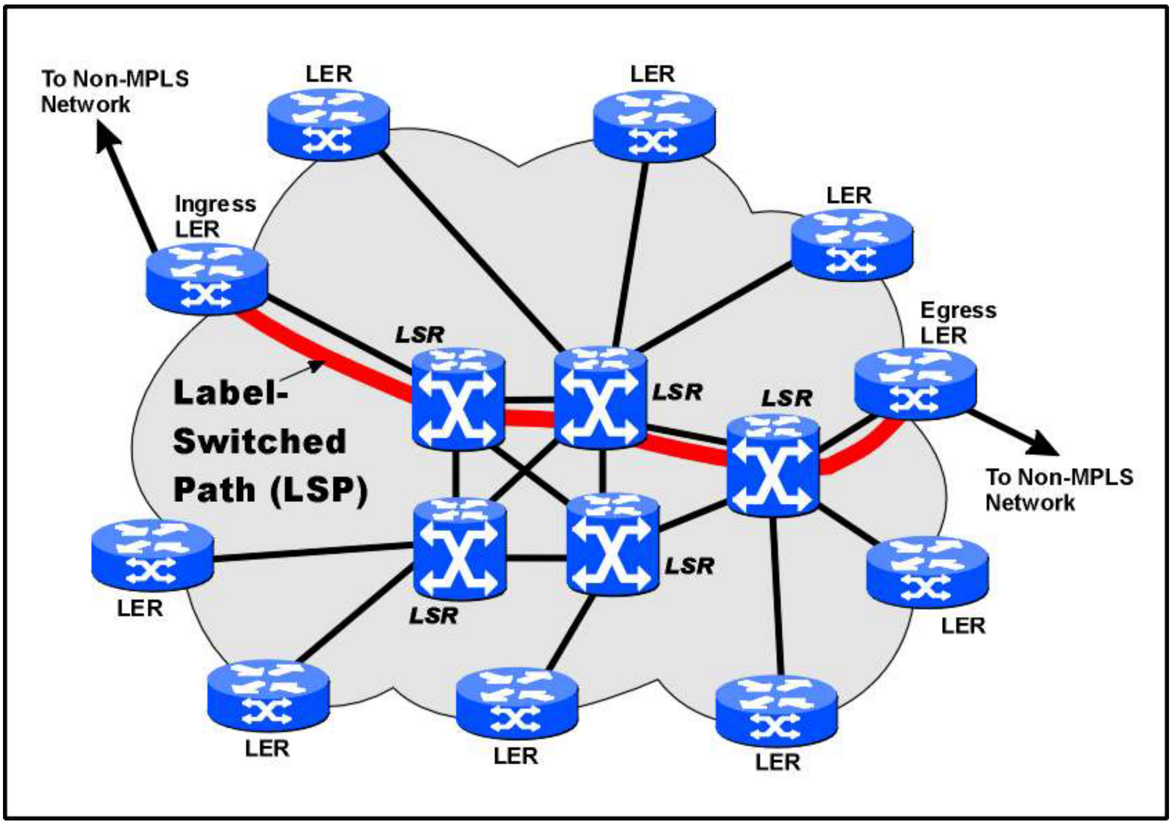



**Figure 71: Traffic Flow in an MPLS Network**

To view statistical information on pseudo-threads (average time of run, maximum time of run, number of times the thread was called, etc.) of MPLS-related routing protocols, refer to the section *MPLS and Routing Performance*, page *771*.

# Label Distribution Protocol (LDP)

## General

The Label Distribution Protocol (LDP) is a protocol for distributing labels among LSRs. It contains a set of procedures and messages by which Label Switching Routers (LSRs) establish Label Switched Paths (LSPs) through a network by mapping network-layer routing information directly to data-link layer switched paths.

LDP associates a Forwarding Equivalence Class (FEC) [RFC3031] with each LSP it creates. The FEC associated with an LSP specifies which packets are "mapped" to that LSP. LDP's hello protocol is UDP-based and is sent periodically. Upon receipt of the hello, LDP establishes a TCP session to the sender. Once established, FEC and label-binding information is exchanged.

LDP uses both UDP and TCP port 646.

## Usage

A minimal LDP configuration requires the following:

- Enabling OSPF protocol that updates the routing table.
- Enabling Router LDP.
- Enabling Label switching and LDP for each interface on which LDP is to be run.

Following is an example of how to set up an OS900 to run LDP.

To configure LDP on interface **`vif2`**:

Example

```
interface vlan vif2
 tag 3
 ip 10.1.7.1/24
 ports 26
 label-switching
 ldp
!
interface dummy dummy1
 ip 3.3.3.3/32
!
router ospf
 ospf router-id 3.3.3.3
 passive-interface dummy1
 network 3.3.3.3/32 area 0
 network 10.1.7.0/24 area 0
!
router ldp
 router-id 3.3.3.3
 transport-address 3.3.3.3 0
!
```

# Traffic Engineering (TE)

## General

Traffic Engineering (TE) can be used to resolve congestion and improve network utilization. Routing protocols usually create a single "shortest path" and all the traffic is sent through that path. The consequence is that the "shortest path" becomes congested while at the same time "longer" paths become underutilized. Now instead of adding more and more bandwidth to avoid congestion, the TE approach is to "put the traffic where the bandwidth is available" see *Figure 72*.

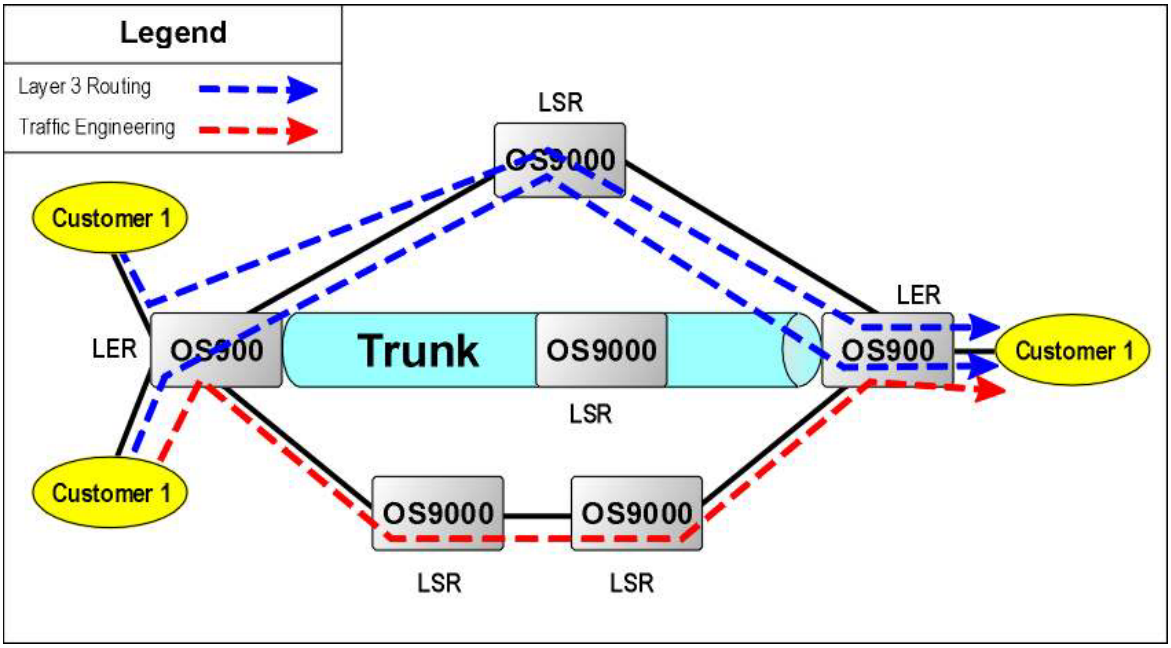



**Figure 72: MPLS Signaling**

MPLS Traffic Engineering allows explicit routing and set-up of LSPs with bandwidth reservation. It also provides control over how LSPs are recovered in the event of failure. Such functionality enables value-added services like Traffic engineered VPNs, Service Level Agreements (SLA) and Multi-media over IP solution (e.g., VoIP).

In order to implement MPLS Traffic Engineering, enhancements were added to the routing protocols and to the MPLS signaling protocols.

The traditional routing protocol has been extended to provide explicit route selection while maintaining predefined constraints. Examples of such constraints are bandwidth requirements, include/exclude nodes, and include/exclude specific links. The goal of constraint-based routing is to compute an optimal path from a given node to another under the constraints.

The enhancements to the MPLS signaling protocols to allow explicit constraint-based routing produced the following extended protocols:

- Resource Reservation Protocol – Traffic Engineering (RSVP-TE)
- Constrained Routing enabled Label Distribution Protocol (CR-LDP).

The enhanced Signaling protocol can provide:

1. Coordinate label distribution
2. Explicit routes (strict & loose)
3. Bandwidth reservation
4. Class of Service
5. Preemption of existing LSPs
6. Loop prevention
7. Protection LSP

Using the above technology and protocols, the OS900 is able to provide many of the new services that Service Providers seek to offer using TE functions. Examples are bandwidth assurance, diverse routing, load balancing, path redundancy, preparation of alternative path for fast recovery, and other services necessary for providing QoS.

As explained in the previous paragraph, the OS900 has the ability to create traffic engineered LSPs called trunks[101]. These trunks can be created using either CR-LDP (LDP trunks) or RSVP-TE (RSVP trunks). An important constraint that the administrator can define for a trunk is the amount of bandwidth needed for the trunk. While the trunk is established, the bandwidth is reserved on all the OS900s along the path. If according to the internal admission control there is not enough bandwidth available on one of the OS900s, that trunk would either fail or replace an existing trunk with lower priority.

After trunk creation, the rate-limit can be configured to police the traffic sent through the trunk and to ensure it does not cross the reserved bandwidth boundary as specified in the trunk definition.

## CR-LDP

Constrained-Routing LDP (CR-LDP) is LDP extended to meet Traffic Engineering requirements in setting up routing paths. For example, an LSP can be set up based on explicit route constraints, QoS constraints, etc.

Following is an example of a trunk configuration using CR-LDP:

The trunk allocates 10 Mbps and is destined to LER with transport address 3.3.3.3 and passes through interior LSRs with transport addresses 1.1.1.1 and 2.2.2.2.

<u>Example</u>

```
ldp-trunk MyTrunk
 primary MyPath
 bandwidth 10m
 to 3.3.3.3
 enable
!
ldp-path MyPath
 1.1.1.1 loose
 2.2.2.2 loose
!
```

## RSVP-TE

The RSVP-TE protocol is an extension of RSVP for establishing LSPs in MPLS networks while meeting traffic engineering requirements. RSVP allows the use of source routing where the ingress

[101] Also called tunnels.

router determines the complete path through the network. The ingress router can use CSPF computation to determine a path to the destination, ensuring that any QoS and TE requirements are met. The resulting path is then used to establish the LSP.

The OS900 RSVP-TE implementation provides smooth rerouting of LSPs, preemption, and loop detection. It can be used for QoS and load balancing across the network core.

RSVP is enabled as shown below:

Example

```
interface vlan vif2
 tag 3
 ip 10.1.5.3/24
 ports 2
 label-switching
 ldp
 rsvp
!
router rsvp
!
router ospf
 ospf router-id 3.3.3.3
 passive-interface dummy1
 network 3.3.3.3/32 area 0
 network 10.1.5.0/24 area 0
 network 10.1.7.0/24 area 0
 te
 cspf
```

Following is an example of a trunk configuration using RSVP-TE:

The trunk allocates 10 Mbps and is destined to LER with transport address 2.2.2.2 and passes through interior LSRs with transport addresses 3.3.3.3.

Example

```
rsvp-trunk t1
 primary path p1
 primary bandwidth 10m
 to 2.2.2.2
!
rsvp-path p1
 3.3.3.3 loose
!
```

# Virtual Circuits

## Definition

A Virtual Circuit (VC) is a point-to-point bi-directional pseudo-wire interconnection for transporting OSI Layer-2 frames of a customer transparently. Several VCs can coexist along a single LSP trunk like wires in a cable as shown in *Figure 73*.


| Ethernet New | Trunk Label | VC Label | User Datagram with Ethernet Header |
|---|---|---|---|

**Figure 73: VCs running through an LSP Trunk**

## Configuration

At *each* of the two VC ends (target LERs), perform the following steps:

1. Enter **`configure terminal`** mode.
2. Set the:
   a. VC name.
   b. VC ID.
   c. IP address on the *primary* target LER at which the VC terminates.
   d. (Optional) *Primary* RSVP trunk name. (If not specified, the OS900 selects between LDP and RSVP-TE.)
   e. (Optional) IPv4 address of the *secondary* target LER for dual-homing.
   f. (Optional) *Secondary* RSVP trunk name. (If not specified, the OS900 selects between LDP and RSVP-TE.)
   g. (Optional) Group ID.
   h. (Optional) Protection mode.

   by invoking the following command:

```
mpls l2-circuit NAME <1-1000000> A.B.C.D [trunk_name TRUNKNAME]
[secondary A.B.C.D] [trunk_name TRUNKNAME] [group_id GROUP_ID]
[protected]
```

where,

**`mpls`**: Set MPLS VC attributes

**`l2-circuit`**: Specify an MPLS Layer-2 VC

**`NAME`**: Identifying string for MPLS Layer-2 VC. (It has local significance only.)

**`<1-1000000>`**: MPLS Layer-2 VC ID. This value is used by LDP to assign a VC label to a packet.

**`A.B.C.D`**: (First appearance) IPv4 address on the target LER at which the VC terminates (LDP transport address of target router)

**`trunk_name`**: (First appearance) Specify *Primary* RSVP Trunk Name

**`TRUNKNAME`**: (First appearance) Identifying string for *Primary* Trunk Name

**`secondary`**: Secondary peer configured for dual homed VC

**`A.B.C.D`**: (Second appearance) IPv4 Address used for the dual-homed

**`trunk_name`**: (Second appearance) Specify *Secondary* Trunk Name

**`TRUNKNAME`**: (Second appearance) Identifying string for *Secondary* Trunk Name

**`group_id`**: Specify group ID

**`GROUPID`**: Group identifier (arbitrary 32-bit value)

**`protected`**: Protect this VC against link failure

> **Note**
>
> If a VC is to go through a CR-LDP or RSVP-TE trunk, it should be destined to the same IP destination as the trunk.

3. Select raw mode (**ethernet**) or tagged mode (**vlan**) for traffic on the VC by invoking the following commands:

   **`action-list NAME`**

   where,

   **`NAME`**: Action list identification up to 20 characters

   **`mpls-action`**

   **`l2-circuit NAME ethernet|vlan`**

   where,

   **`NAME`**: Identifying string for MPLS Layer-2 VC

   **`ethernet`**: Raw mode (without VLAN tag)

   **`vlan`**: Tagged mode (with VLAN tag)

4. Create an ACL enabling packet forwarding and specifying the VC source port by invoking the following commands:

   **`access-list extended WORD`**

   where,

   **`WORD`**: Access-list name

   **`default policy permit`**

   **`src-phy-port eq PORT`**

   where,

   **`PORT`**: Number of VC access port (in VC access interface – see *Figure 74*, page *727*).

5. Specify the IP-based VLAN Interfaces at the MPLS network edge by invoking the following commands:

   **`interface vlan IFNAME`**

   where,

   **`IFNAME`**: Interface ID having the format **`vifX`**, where **`X`** is a decimal number in the range **`1-4095`**.

   **`tag TAG`**

   where,

   **`TAG`**: User-selectable tag (VID) for the VLAN interface. The tag can have any value in the range **`1-4095`**.

   **`ports PORTS-GROUP`**

   where,

   **`PORTS-GROUP`**: Group of ports to be members of the VLAN interface.

   **`ip A.B.C.D/M`**

   where,

   **`A.B.C.D/M`**: IP address/Mask of the VLAN interface.
   The mask can be up to 31 bits long.
   Valid values are up to 223.255.255.254.
   223.255.255.255 is the broadcast value.
   224.0.0.0 to 239.255.255.255 is the multicast range.

   **`label-switching`** (enables label switching on the interface)

   **`ldp`** (enables LDP on this interface)

**rsvp** (*optional*, enables RSVP instead of LDP on this interface. The command is used when the VC is to be directed through an RSVP trunk.)

6. Specify the VLAN Interface at the non-MPLS network that includes the local VC access port by invoking the following commands:

   **interface vlan IFNAME**

   where,

   **IFNAME**: Interface ID having the format **vifX**, where **X** is a decimal number in the range **1-4095**.

   **tag TAG**

   where,

   **TAG**: User-selectable tag (VID) for the VLAN interface. The tag can have any value in the range **1-4095**.

   **ports PORTS-GROUP**

   where,

   **PORTS-GROUP**: Group of ports to be members of the VLAN interface.

7. Bind the ACL to the VLAN Interface at the non-MPLS network by invoking the following command:

   **access-group WORD**

   where,

   **WORD**: Name of the ACL.

8. Specify the interface at which traffic will be received from the remote end of the VC by invoking the following commands:

   **interface dummy IFNAME**

   where,

   **IFNAME**: ID of interface. (The ID must have the format **dummyX**, where **X** can be any integer in the range **1-4095**, e.g., `dummy3000`.)

   **ip A.B.C.D/M**

   where,

   **A.B.C.D/M**: IPv4 address and mask (a.b.c.d/mask). The mask can be up to 31 bits long.

9. Activate OSPF, and specify the router ID and network IP addresses for receiving and transmiting VC traffic by invoking the following commands:

   **router ospf [<0-65535>]**

   where,

   **<0-65535>**: OSPF process ID

   **ospf router-id A.B.C.D**

   where,

   **A.B.C.D**: OSPF router ID in IP address format

   **router-id A.B.C.D**

   where,

   **A.B.C.D**: OSPF router ID in IP address format

   **network A.B.C.D/M area A.B.C.D**

   where,

   **A.B.C.D/M**: IP address of local interface

   **area**: Set the OSPF area ID

   **A.B.C.D**: OSPF area ID in IP address format

   The above command must be repeated for each local interface whose attached network is to participate in the VC – see *Example*, page *727*.

10. Activate LDP, and specify the router ID and transport IP address at the remote end of the VC by invoking the following commands:
    **router ldp**
    **router-id A.B.C.D**
    where,
    **A.B.C.D**: LDP router ID in IP address format
    **transport-address A.B.C.D**
    where,
    **A.B.C.D**: IP Address to be used

## Example

The following example demonstrates configuration of a VC between two OS900s.

At each OS900, one *access* and two *network* interfaces ( one VLAN and one dummy) are configured. A dummy (loopback) interface is specified for each of the two ends of the VC to enable VC traffic flow through the OS900 even if just one VLAN interface having a link to the network exists!

### Network

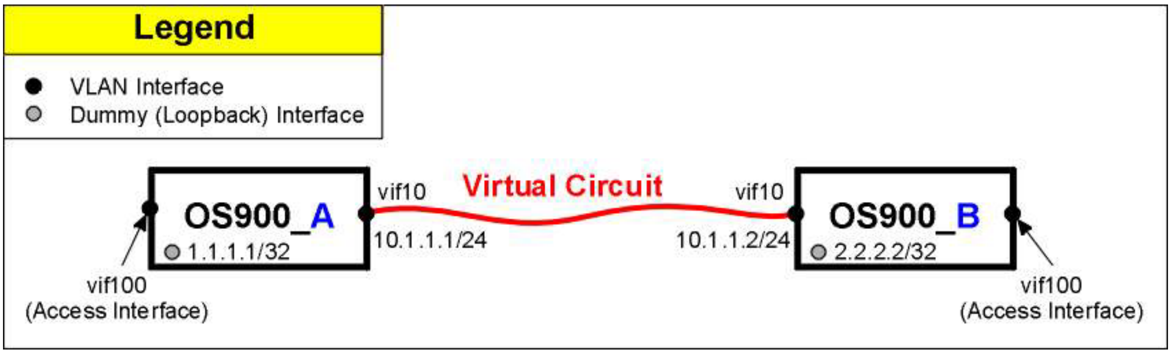



**Figure 74: A Virtual Circuit between Two OS900s**

### Configuration

### OS900_A

```
MRV OptiSwitch 910 version os900-3-0-0-d0736-03-01-08
OS910 login: admin
Password:

OS910> enable
OS910# configure terminal

     -------------------------------Setting VC name and ID, and specifying the IP of its remote end-------------------------------

mpls l2-circuit vc1 20305 2.2.2.2
!
     -----------------------Selecting raw mode (ethernet) or tagged mode (vlan) for traffic on the VC-----------------------

action-list ACL
 mpls-action
  l2-circuit vc1 ethernet
```

```
!
        ----------------------------------------------------------------Creating an ACL----------------------------------------------------------------
access-list extended acl1
        --------------------------------------------------------Enabling packet forwarding--------------------------------------------------------
 default policy permit
 rule 1
  action list ACL
        -------------------------------------------------------Specifying the VC source port-------------------------------------------------------
  src-phy-port eq 1
!
        ------------------------------------Specifying the VLAN Interface at the MPLS network edge------------------------------------
interface vlan vif10
 tag 10
 ip 10.1.1.1/24
 ports 8
 label-switching
 ldp
!
        ---------------Specifying the VLAN Interface at the non-MPLS network that includes the VC source port---------------
interface vlan vif100
 tag 100
 ports 1
        ------------------------------Binding the ACL to the VLAN Interface at the non-MPLS network------------------------------
 access-group acl1
!
        -----------------Specifying the interface at which traffic will be received from the remote end of the VC-----------------
interface dummy dummy1
 ip 1.1.1.1/32
!

        -------Activating OSPF, and specifying the router ID and network IPs for receiving and transmiting VC traffic-------
router ospf
 ospf router-id 1.1.1.1
 network 1.1.1.1/32 area 0
 network 10.1.1.0/24 area 0
!
        --------------Activating LDP, and specifying the router ID and transport IP at the remote end of the VC--------------
router ldp
 router-id 1.1.1.1
```

```
 transport-address 1.1.1.1
```

**OS900_B**

```
MRV OptiSwitch 910 version os900-3-0-0-d0736-03-01-08
OS910 login: admin
Password:

OS910> enable
OS910# configure terminal

   ------------------------------Setting VC name and ID, and specifying the IP of its remote end-------------------------------

mpls l2-circuit vc1 20305 1.1.1.1
!
   ----------------------Selecting raw mode (ethernet) or tagged mode (vlan) for traffic on the VC----------------------

action-list ACL
 mpls-action
  l2-circuit vc1 ethernet
!
   -------------------------------------------------------------Creating an ACL-------------------------------------------------------------

access-list extended acl1

   ------------------------------------------------------Enabling packet forwarding------------------------------------------------------

 default policy permit
 rule 1
  action list ACL

   -----------------------------------------------------Specifying the VC source port-----------------------------------------------------

  src-phy-port eq 1
!
   -----------------------------------Specifying the VLAN Interface at the MPLS network edge-----------------------------------

interface vlan vif10
 tag 10
 ip 10.1.1.2/24
 ports 8
 label-switching
 ldp
!
   --------------Specifying the VLAN Interface at the non-MPLS network that includes the VC source port--------------

interface vlan vif100
 tag 100
 ports 1
```

```
------------------------------Binding the ACL to the VLAN Interface at the non-MPLS network------------------------------

 access-group acl1
!

-----------------Specifying the interface at which traffic will be received from the remote end of the VC-----------------

interface dummy dummy1
 ip 2.2.2.2/32
!

-------Activating OSPF, and specifying the router ID and network IPs for receiving and transmiting VC traffic-------

router ospf
 ospf router-id 2.2.2.2
 network 2.2.2.2/32 area 0
 network 10.1.1.0/24 area 0
!

--------------Activating LDP, and specifying the router ID and transport IP at the remote end of the VC--------------

router ldp
 router-id 2.2.2.2
 transport-address 2.2.2.2
```

## Deleting

To delete a VC:

1. Enter **`configure terminal`** mode
2. Invoke the command:

   **`no mpls l2-circuit NAME <1-1000000> A.B.C.D [secondary A.B.C.D]`**

   where,

   **`NAME`**: Identifying string for MPLS Layer-2 VC.
   **`<1-1000000>`**: MPLS Layer-2 VC ID.
   **`A.B.C.D`**: (First appearance) IPv4 address on the target LER at which the VC terminates (LDP transport address of target router)
   **`secondary`**: Secondary peer configured for dual homed VC
   **`A.B.C.D`**: (Second appearance) IPv4 Address used for the dual-homed

## Operability

### Independency

By default, the VC AC (Attachment Circuit) can be operational independent of the MPLS access port's link state – whether UP or DOWN.

To enable the VC AC to be operational independent of the MPLS access port's link state:

1. Enter **`configure terminal`** mode
2. Invoke the command:

   **`no mpls l2-circuit NAME regards-ac-state`**

   where,

   **`NAME`**: Identifying string for MPLS Layer-2 VC.

### Dependency

To make the UP state mandatory for the VC AC to be operational:

1. Enter **`configure terminal`** mode
2. Invoke the command:

   **`mpls l2-circuit NAME regards-ac-state`**

   where,

   **`NAME`**: Identifying string for MPLS Layer-2 VC.

## Status

In previous OS900 versions, a 'label withdrawn' packet was sent for each change in the status of a pseudowire (PW). In this version, by default, the status of a pseudowire is announced according to RFC 4447. In this mode, additional information is supplied to describe the VC state using PW-Status packets.

### Legacy

To set the OS900 to send 'label withdrawn' packets:

1. Enter **`configure terminal`** mode
2. Enter router mode by invoking the command:

   **`router ldp`**
3. Invoke the command:

   **`targeted-peer A.B.C.D pw-status-disable`**

   where,

   **`A.B.C.D`**: IPv4 address on the target LER at which the VC terminates (LDP transport address of target router).

### RFC 4447

To set the OS900 to send 'PW-Status' packets per the RFC 4447:

1. Enter **`configure terminal`** mode
2. Enter router mode by invoking the command:

   **`router ldp`**
3. Invoke the command:

   **`no targeted-peer A.B.C.D pw-status-disable`**

   where,

   **`A.B.C.D`**: IPv4 address on the target LER at which the VC terminates (LDP transport address of target router).

## Virtual Port-Link Reflection

This is a proprietary MRV feature. The feature's mechanism functions like the Link Reflection mechanism (described in the section *Link Reflection* on page *146*) except that it operates over a VC between two OS900s interconnected *across an MPLS cloud*. It causes the link to an access port at *one* end of the VC to go DOWN if the link to the access port at the *other* end of the VC is brought down.

This feature solves deadlock scenarios in the spanning tree topology.

### Enabling

By default, Virtual Port-Link Reflection is disabled.

To enable Virtual Port-Link Reflection:

1. Enter **`configure terminal`** mode
2. Invoke the command:

   **`mpls l2-circuit virtual-port-reflection`**

Example

```
R2(config)# mpls l2-circuit virtual-port-reflection
R2(config)#
```

**Disabling**

To disable Virtual Port-Link Reflection:

1. Enter **configure terminal** mode
2. Invoke the command:
   **no mpls l2-circuit virtual-port-reflection**

Example

```
R2(config)# no mpls l2-circuit virtual-port-reflection
R2(config)#
```

# MPLS DiffServ

MPLS DiffServ provides the following:

1. Bandwidth reservation for CR-LDP and RSVP-TE trunks.
2. Policing MPLS VPN bandwidth reservation.
3. Support for E-LSPs[102].
4. Option to map DSCP bits to MPLS EXP bits.
5. Option to map VPT bits to MPLS EXP bits.
6. EXP bits are marked on both Trunk and VC labels (important for PHP).
7. VC ingress/egress accounting.

An important feature of the OS900 is its ability to provide differentiated service levels to specific flows that use the *same* Virtual Circuit (VC).

By default, the VPT bits of an ingress frame at an OS900 LER are mapped to MPLS EXP bits of the MPLS header.

To enable marking of the *EXP* bits of a frame according to the DSCP value for the group of ports invoke the command **port qos-trust PORTS-GROUP|all l2|l2l3|l3|port** (described in the section *Selecting an SL Criterion*, page *282*).

[102] An E-LSP is an LSP on which routers (LER or LSR) provide QoS handling of MPLS packets according to the EXP field in the MPLS header. Since the EXP field is 3 bits long, up to $2^3$ (eight) classes of traffic can be defined. This allows for up to 8 classes of traffic using the same label to be concurrently carried over a *single* LSP.

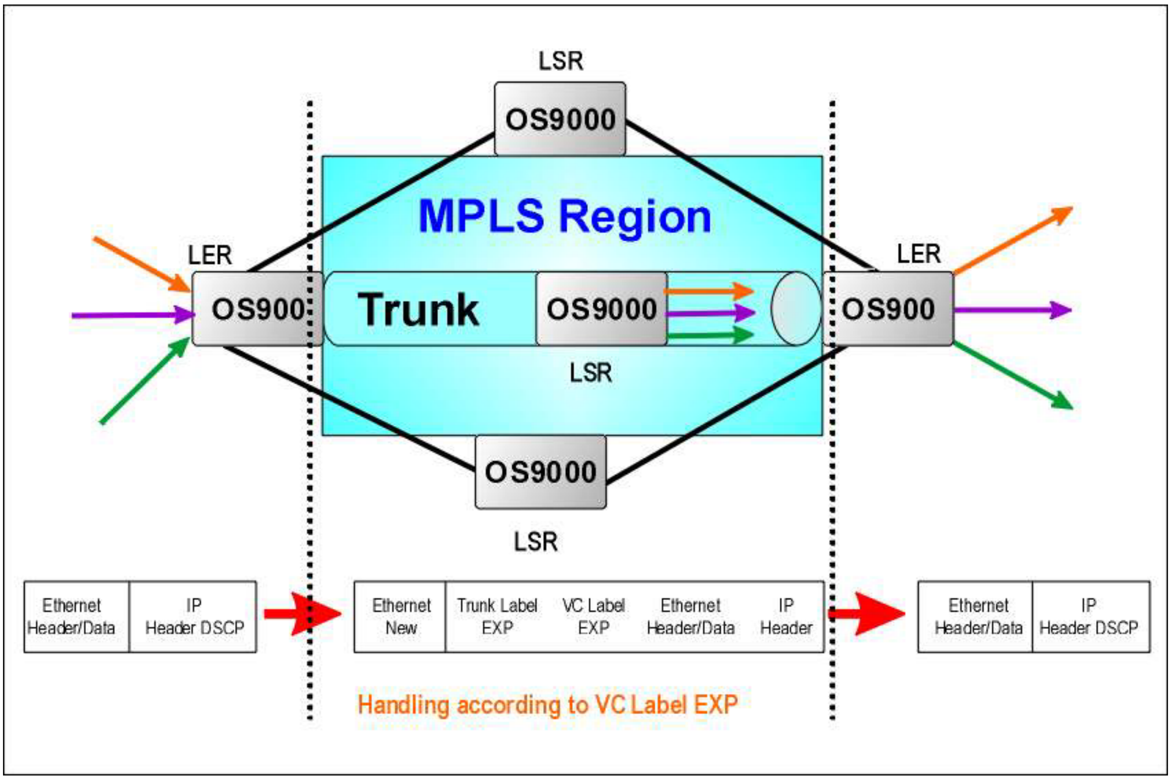



**Figure 75: MPLS and QoS Functionality**

By default, priority is based on the *Layer 2 VPT* value of ingress and egress packets.
An SL (diffserv service level – see *DiffServ Service Levels*, page *281*) is assigned to an MPLS packet according to the following correlation:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **VPT** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **SL** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

# Viewing Commands

MPLS information can be viewed by invoking the following commands:

## Cross-connect Table

To view the MPLS Cross-connect table:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`show mpls cross-connect-table`**

   where,

   **`mpls`**: Configure MPLS specific attributes

   **`cross-connect-table`**: MPLS Cross-connect table

Example

```
R2# show mpls cross-connect-table
  Cross connect ix: 1, in intf: -, in label: 0, out-segment ix: 1
    Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 1, owner: RSVP, out intf: vif4011, out label: 640
    Nexthop addr: 192.170.1.3, cross connect ix: 1, op code: Push

  Cross connect ix: 2, in intf: vif4010, in label: 1282, out-segment ix: 2
    Owner: LDP VC, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 2, owner: LDP VC, out intf: vif2, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 2, op code: Pop for VC

  Cross connect ix: 3, in intf: vif4010, in label: 1283, out-segment ix: 3
    Owner: LDP VC, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 3, owner: LDP VC, out intf: vif3, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 3, op code: Pop for VC
```

## Forwarding Table

To view the MPLS *Forwarding* table:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls forwarding-table**

   where,

   **mpls**: Configure MPLS specific attributes

   **forwarding-table**: MPLS Forwarding table

Example

```
R2# show mpls forwarding-table
Codes: > - selected FTN, B - BGP FTN, C - CR-LDP FTN, K - CLI FTN,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, U - unknown FTN

Code  FEC                 Nexthop             Out-Label  Out-Intf
R>    1.1.1.1/32          192.170.1.3         640        vif4011
L     1.1.1.1/32          192.168.1.1         3          vif4010
L>    3.3.3.3/32          192.170.1.3         3          vif4011
L>    192.169.1.0/24      192.168.1.1         3          vif4010
```

## FTN Table

To view the MPLS FTN table:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls ftn-table**

   where,

   **mpls**: Configure MPLS specific attributes

   **ftn-table**: MPLS FEC-To-NHLFE table. The table (stored in LERs) contains maps of Destination IP addresses to MPLS labels for ingress packets.

Example

```
R2# show mpls ftn-table
 Primary FTN entry with FEC: 1.1.1.1/32, ix 3, row status: Active
  Owner: RSVP, Action-type: Redirect to Tunnel, Exp-bits: 0x0
  Resource_id: 30
  Description: T1
  Cross connect ix: 1, in intf: -, in label: 0, out-segment ix: 1
    Owner: RSVP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 1, owner: RSVP, out intf: vif4011, out label: 640
    Nexthop addr: 192.170.1.3, cross connect ix: 1, op code: Push

 Non-primary FTN entry with FEC: 1.1.1.1/32, ix 1, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0
  Resource_id: 0
  Description: N/A
  Cross connect ix: 1003, in intf: -, in label: 0, out-segment ix: 1003
    Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 1003, owner: LDP, out intf: vif4010, out label: 3
    Nexthop addr: 192.168.1.1, cross connect ix: 1003, op code: Swap

 Primary FTN entry with FEC: 3.3.3.3/32, ix 4, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0
  Resource_id: 0
  Description: N/A
  Cross connect ix: 1004, in intf: -, in label: 0, out-segment ix: 1004
    Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 1004, owner: LDP, out intf: vif4011, out label: 3
    Nexthop addr: 192.170.1.3, cross connect ix: 1004, op code: Swap

 Primary FTN entry with FEC: 192.169.1.0/24, ix 2, row status: Active
  Owner: LDP, Action-type: Redirect to Tunnel, Exp-bits: 0x0
  Resource_id: 0
  Description: N/A
  Cross connect ix: 1003, in intf: -, in label: 0, out-segment ix: 1003
    Owner: LDP, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 1003, owner: LDP, out intf: vif4010, out label: 3
    Nexthop addr: 192.168.1.1, cross connect ix: 1003, op code: Swap
```

## ILM Table

To view the MPLS ILM table:

1. Enter **enable** mode.
2. Invoke the command:

**show mpls ilm-table**

where,

**mpls**: Configure MPLS specific attributes

**ilm-table**: MPLS Incoming Label Map table. The table (stored in LSRs) contains maps of ingress packet MPLS labels to egress packet MPLS labels for LSPs.

Example

```
R2# show mpls ilm-table
In-Label   Out-Label  In-Intf    Out-Intf   Nexthop         FEC
640        0          vif4010    vif640     0.0.0.0         0.0.2.128/32
641        0          vif4010    vif641     0.0.0.0         0.0.2.129/32
642        0          vif4010    vif642     0.0.0.0         0.0.2.130/32
643        0          vif4010    vif643     0.0.0.0         0.0.2.131/32
644        0          vif4010    vif644     0.0.0.0         0.0.2.132/32
645        0          vif4010    vif645     0.0.0.0         0.0.2.133/32
646        0          vif4010    vif646     0.0.0.0         0.0.2.134/32
647        0          vif4010    vif647     0.0.0.0         0.0.2.135/32
648        0          vif4010    vif648     0.0.0.0         0.0.2.136/32
```

## In-segment Table

To view the MPLS In-segment table:

1. Enter **enable** mode.
2. Invoke the command:
   **show mpls in-segment-table**
   where,
   **mpls**: Configure MPLS specific attributes
   **in-segment-table**: MPLS In-segment table.

Example

```
R2# show mpls in-segment-table
 In-segment entry with in label: 640, in intf: vif4010, row status: Active
  Owner: LDP VC, # of pops: 1, fec: 0.0.2.128/32
  Cross connect ix: 641, in intf: vif4010, in label: 640, out-segment ix: 641
    Owner: LDP VC, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 641, owner: LDP VC, out intf: vif640, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 641, op code: Pop for VC

 In-segment entry with in label: 641, in intf: vif4010, row status: Active
  Owner: LDP VC, # of pops: 1, fec: 0.0.2.129/32
  Cross connect ix: 642, in intf: vif4010, in label: 641, out-segment ix: 642
    Owner: LDP VC, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 642, owner: LDP VC, out intf: vif641, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 642, op code: Pop for VC

 In-segment entry with in label: 642, in intf: vif4010, row status: Active
  Owner: LDP VC, # of pops: 1, fec: 0.0.2.130/32
  Cross connect ix: 643, in intf: vif4010, in label: 642, out-segment ix: 643
    Owner: LDP VC, Persistent: No, Admin Status: Up, Oper Status: Up
   Out-segment with ix: 643, owner: LDP VC, out intf: vif642, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 643, op code: Pop for VC
```

## Out-segment Table

To view the MPLS Out-segment table:

1. Enter **enable** mode.
2. Invoke the command:
   **show mpls out-segment-table**
   where,
   **mpls**: Configure MPLS specific attributes
   **out-segment-table**: MPLS Out-segment table.

Example

```
R2# show mpls out-segment-table
   Out-segment with ix: 2, owner: LDP VC, out intf: vif2, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 2, op code: Pop for VC

   Out-segment with ix: 3, owner: LDP VC, out intf: vif3, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 3, op code: Pop for VC

   Out-segment with ix: 4, owner: LDP VC, out intf: vif4, out label: 0
    Nexthop addr: 0.0.0.0, cross connect ix: 4, op code: Pop for VC
```

## L2 Circuits

To view the MPLS Layer 2 Circuit:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls l2-circuit**

   where,

   **mpls**: Configure MPLS specific attributes

   **l2-circuit**: MPLS Layer-2 Virtual Circuit data.

Example

```
R2# show mpls l2-circuit
MPLS Layer-2 Virtual Circuit: VC2, id: 2
 Endpoint: 1.1.1.1
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: vif2, Port 1
 Virtual Circuit Type: Ethernet VLAN
MPLS Layer-2 Virtual Circuit: VC3, id: 3
 Endpoint: 1.1.1.1
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: vif3, Port 1
 Virtual Circuit Type: Ethernet VLAN
MPLS Layer-2 Virtual Circuit: VC4, id: 4
 Endpoint: 1.1.1.1
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: vif4, Port 1
 Virtual Circuit Type: Ethernet VLAN
```

## L2 Circuit Groups

To view the MPLS Layer 2 Circuit Group:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls l2-circuit-group**

   where,

   **mpls**: Configure MPLS specific attributes

   **l2-circuit-group**: MPLS Layer-2 Virtual Circuit group data.

Example

```
R2# show mpls l2-circuit-group
MPLS Layer-2 Virtual Circuit Group: 1, id: 1
 Virtual Circuits configured:
  1. VC1000
```

## LDP Parameters

To view the MPLS LDP information:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls ldp**

   where,

   **mpls**: Configure MPLS specific attributes

   **ldp**: Label Distribution Protocol (LDP).

Example

```
R2# show mpls ldp parameter
Router ID                 : 2.2.2.2
LDP Version               : 1
Global Merge Capability   : N/A
Label Advertisement Mode  : Downstream Unsolicited
Label Retention Mode      : Liberal
Label Control Mode        : Independent
Loop Detection            : Off
Loop Detection Count      : 0
Request Retry             : Off
Propagate Release         : Disabled
Hello Interval            : 5
Targeted Hello Interval   : 15
Hold time                 : 15
Targeted Hold time        : 45
Keepalive Interval        : 10
Keepalive Timeout         : 30
Request retry Timeout     : 5
Targeted Hello Receipt    : Disabled
Transport Address data    :
  Labelspace 0            : 2.2.2.2 (in use)
Import BGP routes         : No
PHP mode                       : Yes
Global MTU                      : 0
MD5 mode                        : Off
```

## VC Table

To view the MPLS VC table:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls vc-table**

   where,

   **mpls**: Configure MPLS specific attributes

   **vc-table**: MPLS Virtual Circuit table.

Example

```
R2# show mpls vc-table
VC-ID     In Intf   Out Intf  Out Label  Nexthop         Status
2         vif2      vif4010   1280       1.1.1.1         Active
3         vif3      vif4010   1281       1.1.1.1         Active
4         vif4      vif4010   1282       1.1.1.1         Active
5         vif5      vif4010   1283       1.1.1.1         Active
6         vif6      vif4010   1284       1.1.1.1         Active
7         vif7      vif4010   1285       1.1.1.1         Active
8         vif8      vif4010   1286       1.1.1.1         Active
9         vif9      vif4010   1287       1.1.1.1         Active
10        vif10     vif4010   1288       1.1.1.1         Active
```

### Administrative Groups

To view the MPLS Administrative Groups:

1. Enter **`enable`** mode.
2. Invoke the command:

    **`show mpls admin-groups`**

    where,

    **`mpls`**: Configure MPLS specific attributes

    **`admin-groups`**: Administrative Groups. Each administrative group is designated (at the local router) by an ID in the range 0-31. The ID represents one or more interfaces. The ID is distributed to all the other routers in the MPLS network if TE is activated (by selecting CR-LDP or RSVP-TE).

Example

```
R2# show mpls admin-groups
 Admin group detail:
  Value of 1 associated with admin group 'G1'
```

### Mapped Routes

To view the MPLS Mapped Routes:

1. Enter **`enable`** mode.
2. Invoke the command:

    **`show mpls mapped-routes`**

    where,

    **`mpls`**: Configure MPLS specific attributes

    **`mapped-routes`**: Mapped MPLS routes. Shows subnets assigned to each MPLS label. The command can be used to save on MPLS labels.

Example

```
R2# show mpls mapped-routes
Mapped-route        IPv4 FEC
192.170.1.3/32      3.3.3.3/32
```

# Configuration Commands

## MPLS Route Map

#### Creating

To create an IP4 Route Map:

1. Enter **`configure terminal`** mode.
2. Invoke either of the following equivalent commands:

    **`mpls map-route A.B.C.D A.B.C.D A.B.C.D A.B.C.D`**

    **`mpls map-route A.B.C.D/M A.B.C.D/M`**

    where,

    **`mpls`**: Configure MPLS specific attributes

    **`map-route`**: Map an IPv4 route

    **`A.B.C.D`**: (first appearance) IPv4 prefix to be mapped

    **`A.B.C.D`**: (second appearance) Mask for IPv4 address to be mapped. The mask can be up to 31 bits long.

    **`A.B.C.D`**: (third appearance) IPv4 Forwarding Equivalence Class to which route is to be mapped

    **`A.B.C.D`**: (fourth appearance) Mask for IPv4 Forwarding Equivalence Class to which route is to be mapped. The mask can be up to 31 bits long.

    **`A A.B.C.D/M`**: (first appearance) IPv4 prefix with mask to be mapped

**A A.B.C.D/M**: (second appearance) IPv4 Forwarding Equivalence Class to which route is to be mapped with mask

Example

```
R2(config)# mpls map-route 192.170.1.3 192.170.1.0 192.169.1.254 192.169.1.0
R2(config)#
```

### Deleting

To delete an IP4 Route Map:

1. Enter **configure terminal** mode.
2. Invoke either of the following equivalent commands:

   **mpls map-route A.B.C.D A.B.C.D A.B.C.D A.B.C.D**

   **mpls map-route A.B.C.D/M A.B.C.D/M**

   where,

   **mpls**: Configure MPLS specific attributes

   **map-route**: Map an IPv4 route

   **A.B.C.D**: (first appearance) IPv4 prefix to be mapped

   **A.B.C.D**: (second appearance) Mask for IPv4 address to be mapped. The mask can be up to 31 bits long.

   **A.B.C.D**: (third appearance) IPv4 Forwarding Equivalence Class to which route is to be mapped

   **A.B.C.D**: (fourth appearance) Mask for IPv4 Forwarding Equivalence Class to which route is to be mapped. The mask can be up to 31 bits long.

   **A A.B.C.D/M**: (first appearance) IPv4 prefix with mask to be mapped

   **A A.B.C.D/M**: (second appearance) IPv4 Forwarding Equivalence Class to which route is to be mapped with mask

Example

```
R2(config)# no mpls map-route 192.170.1.3 192.170.1.0 192.169.1.254 192.169.1.0
R2(config)#
```

## Upper-limit MPLS Labels

### Setting

To set the maximum value for an MPLS Label:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **mpls max-label-value <16-1048575>**

   where,

   **mpls**: Configure MPLS specific attributes

   **max-label-value**: Specify a maximum label value

   **<16-1048575>**: Maximum size to be used for all label pools

Example

```
R2(config)# mpls max-label-value 10000
R2(config)#
```

### Clearing

To clear the maximum value for an MPLS Label:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no mpls max-label-value**

Example

```
R2(config)# no mpls max-label-value
% Operation will take affect only after reboot.
R2(config)#
```

## Lower-limit MPLS Labels

### Setting

To set the minimum value for an MPLS Label:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **mpls min-label-value <16-1048575>**
   where,
   **mpls**: Configure MPLS specific attributes
   **min-label-value**: Specify a minimum label value
   **<16-1048575>**: Minimum size to be used for all label pools

Example

```
R2(config)# mpls min-label-value 100
R2(config)#
```

### Clearing

To clear the minimum value for an MPLS Label:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no mpls min-label-value**

Example

```
R2(config)# no mpls min-label-value
% Operation will take affect only after reboot.
R2(config)#
```

## LDP Path

### Creating

To create an LDP path:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **ldp-path PATHNAME**
   where,
   **PATHNAME**: Name to be used for path

Example

```
R2(config)# ldp-path P1
R2(config-path)#
```

### Deleting

To delete an LDP path:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no ldp-path PATHNAME**
   where,
   **PATHNAME**: Name to be used for path

Example

```
R2(config-path)# no ldp-path P1
R2(config)#
```

## LDP Trunk (Group)

### Creating

To create an LDP trunk:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **ldp-trunk TRUNKNAME**
   **TRUNKNAME**: Name to be used for trunk

Example

```
R2(config)# ldp-trunk T1
R2(config-trunk)#
```

### Deleting

To delete an LDP trunk:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **ldp-trunk TRUNKNAME**
   **TRUNKNAME**: Name to be used for trunk

Example

```
R2(config)# no ldp-trunk T1
R2(config)#
```

## RSVP Path

### Creating

To create an RSVP path:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **rsvp-path PATHNAME**
   where,
   **PATHNAME**: Name to be used for path

Example

```
R2(config)# rsvp-path P1
R2(config-path)#
```

### Deleting

To delete an RSVP path:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no rsvp-path PATHNAME**
   **PATHNAME**: Name to be used for path

Example

```
R2(config)# no rsvp-path P1
R2(config)#
```

## RSVP Trunk (Group)

### Creating

To create an RSVP trunk:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **rsvp-trunk TRUNKNAME**
   **TRUNKNAME**: Name to be used for trunk

Example

```
R2(config)# rsvp-trunk T1
R2(config-trunk)#
```

#### Deleting

To delete an RSVP trunk:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no rsvp-trunk TRUNKNAME**
   **TRUNKNAME**: Name to be used for trunk

Example

```
R2(config)# no rsvp-trunk T1
R2(config)#
```

### MPLS Activeness

#### Activating

To activate MPLS, select a routing protocol as follows:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **router ldp|rsvp**

Example 1

```
R2(config)# router ldp
R2(config-router)#
```

Example 2

```
R2(config)# router rsvp
R2(config-router)#
```

#### Deactivating

To deactivate MPLS, select a routing protocol as follows:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **router ldp|rsvp**

Example 1

```
R2(config)# no router rsvp
This will erase all RSVP-PATHs and RSVP-TRUNKs configured. Do you want to continue? T
ype [y/n]: y
R2(config)#
```

### Administrative Group

#### Creating

To create an Administrative Group:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **mpls admin-group NAME <0-31>**
   where,
   **mpls**: Configure MPLS specific attributes

**admin-group**: Add a new Administrative Group
**NAME**: Name of administrative group to be added
**<0-31>**: Value of administrative group to be added

Example

```
R2(config)# mpls admin-group G2 2
R2(config)#
```

**Deleting**

To delete an Administrative Group:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no mpls admin-group NAME <0-31>**
   where,
   **mpls**: Configure MPLS specific attributes
   **admin-group**: Add a new Administrative Group
   **NAME**: Name of administrative group to be added
   **<0-31>**: Value of administrative group to be added

Example

```
R2(config)# no mpls admin-group G2 2
R2(config)#
```

# Hierarchical VPLS (H-VPLS)

## General

A Hierarchical VPLS (H-VPLS) is a VPLS constructed in two tiers of differing hierarchy. The tiers are interconnected with one or more VCs[103] – see *Figure 76*, page *746*. The first tier, which is the VPLS core/hub, consists of a full mesh[104] of devices having routing and bridging capabilities. Such devices are referred to as PE-rs. The second tier, which is the VPLS edge/spoke, can consist of OS900s.

H-VPLS complies to *draft ietf-l2vpn-vpls-ldp*. (Draft 9 has been released.)

## Purpose

H-VPLS is proposed to overcome the drawbacks of regular VPLS that arise in expanding and large scale deployments. Among these drawbacks are:

1. The need to configure all the PEs for each new device to be added in the network.
2. Bandwidth consumption by signaling packets between each pair of PEs in the VPLS domain
3. Packet replication requirement
4. Recovery/convergence time in case of failure of a VC.

## Advantages

The H-VPLS model has the following advantages over regular VPLS:

1. Only one VC is required to connect an OS900 to a PE-rs in the VPLS domain as opposed to a mesh of VCs as would be required if the network was totally VPLS.
2. As the need arises, new CEs can be connected to the VPLS network by simply connecting each OS900 (to which the CEs are attached) to a PE-rs in the VPLS domain with a VC.

[103] Pseudo wires

[104] A full mesh is direct connection of each and every device to each and every of the other devices.

## Principle of Operation

All traffic going from/to CEs to/from one of the PE-rs devices in the VPLS domain will go through a VC. An OS900 needs only to be aware of the specific PE-rs (in the VPLS domain) to which it is connected although it is participating in the VPLS service that spans multiple devices.

## Dual Homing (Redundant Spoke Connection)

Having just one VC between an OS900 and a PE-rs is risky because if this connection fails the CEs connected to the OS900 are completely disconnected from the VPLS domain.

To address this potential problem, the *dual-homing* option can be used. In this option, an OS900 is connected via two VCs to two PE-rs devices in the same VPLS domain – see *Figure 76*, page *746*. One VC (Primary VC) remains active while the other VC (Secondary VC) remains in standby; ready to take over the tasks of the Primary VC in case the latter fails.

## Application

The H-VPLS model enables the service provider to extend the VPLS domains by placing cost-effective OS900s in multi-tenant buildings and aggregating them to a PE-rs in a large central office (CO) facility – see *Figure 76*, page *746*. Using dual VCs instead of one provides connectivity-redundancy protection.

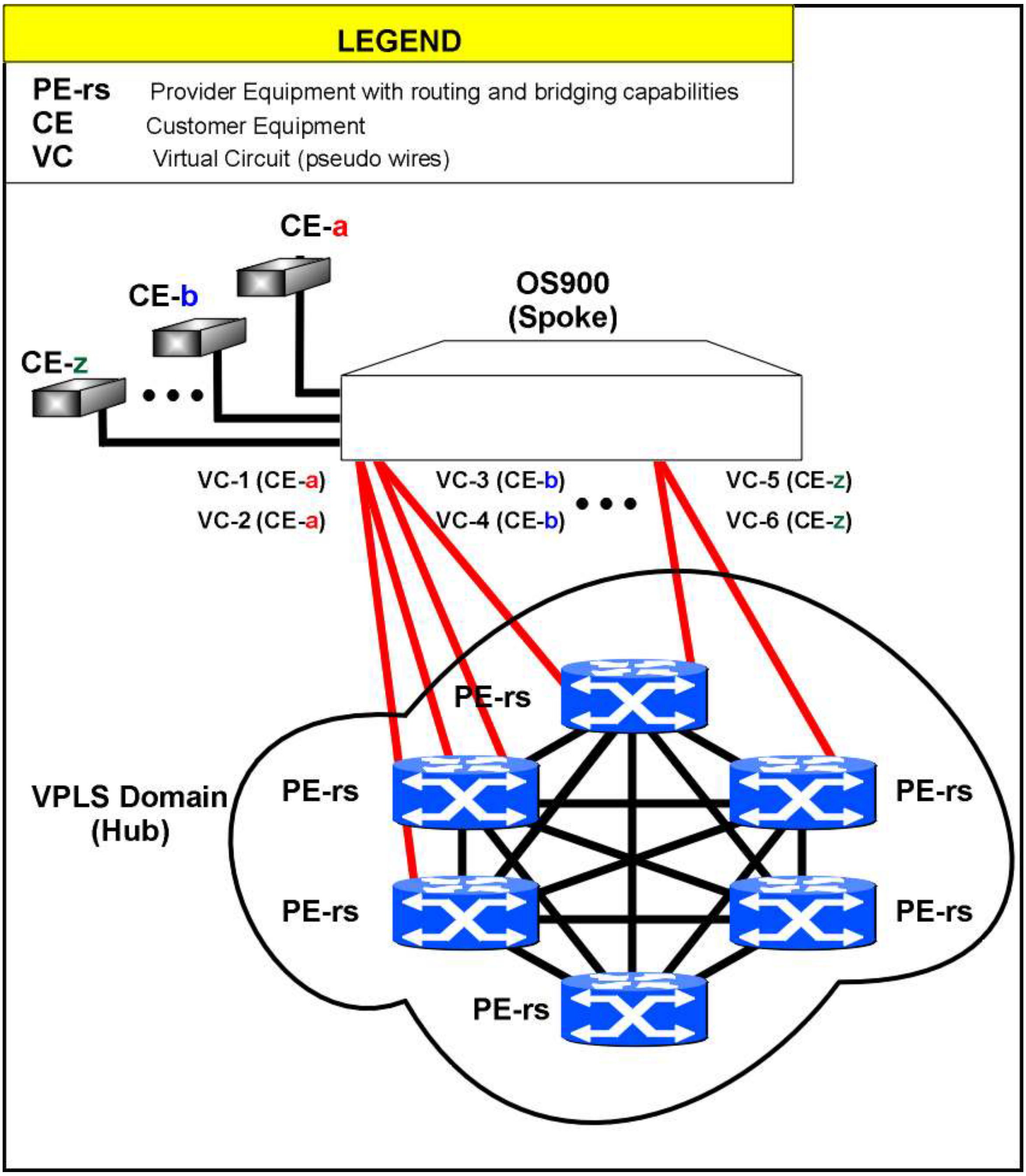



**Figure 76: H-VPLS Network**

## Configuration

The procedure for configuring an OS900 to operate in single-homing mode or dual-homing mode is as follows:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **mpls l2-circuit NAME ID A.B.C.D secondary A.B.C.D**

   where,

   **NAME**: Name for VC. (It applies only locally.)

   **ID**: ID of primary VC. The ID may be set as any number in the range 1-1000000. (It must be identical to the VPLS ID to which this VC is to connect.)

   **A.B.C.D**: (first appearance) IP address of PE-rs to which the primary VC is to connect.

**A.B.C.D**: (second appearance) It applies only for dual-homing mode. IP address of a *different* PE-rs to which the secondary VC is to connect. (The secondary VC becomes active only when the primary VC fails.)

Example

```
OS900> enable
OS900# configure terminal
OS900(config)# mpls l2-circuit Sales_VC 500 2.2.2.2 secondary 3.3.3.3
OS900(config)#
```

## Viewing

To view the configuration:

1. Enter **enable** mode.
2. Invoke the command:

   **show mpls l2-circuit**

   where,

   **NAME**: Name for VC. (It applies only locally.)

Example

```
OS900(config)# exit
OS900# show mpls l2-circuit Sales_VC

MPLS Layer-2 Virtual Circuit: Sales_VC, id: 500, priority: primary
 Endpoint: 2.2.2.2
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: vif500, Port: 1
 Virtual Circuit Type: Ethernet VLAN
 Bound to trunk: no trunk, regular LDP usage.
MPLS Layer-2 Virtual Circuit: Sales_VC, id: 500, priority: secondary
 Endpoint: 3.3.3.3
 Control Word: 0
 MPLS Layer-2 Virtual Circuit Group: none
 Bound to interface: vif500, Port: 1
 Virtual Circuit Type: Ethernet VLAN
 Bound to trunk: no trunk, regular LDP usage.
```

# LSP PING

## General

MPLS LSP PING is a tool that enables the user to detect synchronization problems between the MPLS control plane and its associated data plane. Specifically, it can be used to determine if an LSP is set at the control plane level and, more importantly, if the LSP can actually deliver user traffic.

This tool emulates the behavior of the regular ICMP-based PING function by sending MPLS Echo Request packets to a specific FEC. The packets are sent along the same data path as other packets in the FEC. An MPLS Echo Request also carries MRV implementation of LSP PING and is compatible with RFC 4379 entitled *Detecting MPLS Data Plane Failures*.

## LSP PING over a Regular LDP LSP

To run LSP PING over a regular LDP LSP:

1. Enter **enable** mode.
2. Invoke the command:

   **ping mpls ipv4 A.B.C.D/M [repeat <1-65535>] [timeout <1-10>]**

   where,

**ipv4**: MPLS LDP-IPv4 echo message.
**A.B.C.D/M**: IPv4 host/network of the LDP FEC for which the MPLS echo packet is to be generated.
**repeat**: Repeat PING.
**<1-65535>**: Number of times. Default: 5.
**timeout**: Set the maximum wait time between consecutive echo requests.
**<1-10>**: Time in seconds. Default: 5.

## LSP PING over an RSVP-TE LSP

To run LSP PING over an RSVP-TE LSP:

1. Enter **enable** mode.
2. Invoke the command:

```
ping mpls traffic-eng trunkname TRUNKNAME [repeat <1-65535>]
[timeout <1-10>]
```

where,
**traffic-eng**: MPLS RSVP-TE echo message
**trunkname**: Identify RSVP-TE destination by Trunk Name
**TRUNKNAME**: RSVP-TE Trunk Name
**repeat**: Repeat PING.
**<1-65535>**: Number of times. Default: 5.
**timeout**: Set the maximum wait time between consecutive echo requests.
**<1-10>**: Time in seconds. Default: 5.

## Stopping

To stop an LSP PING process:

1. Enter **enable** mode.
2. Invoke the command:

```
ping mpls stop
```

## Replies

Possible LSP PING/Traceroute replies and their significances are as follows:

| LSP PING/Traceroute Reply | Significance |
|---|---|
| `'!' - success:` | The MPLS echo packet succeeded in reaching its destination address/trunkname (specified by the FEC in the ping/traceroute command).<br>The reply could typically include the message:<br>`! 100.2.1.3, return code: 3 (Replying router is FEC egress at stack depth <1>), rtt=29.0 ms` |
| `'R' - downstream router but not destination:` | The transit LSR has found no problem and its data and control planes are synchronized. (`'R'` should appear only when MPLS traceroute is invoked and when a transit LSR replies.)<br>The reply could typically include the message:<br>`R 100.2.1.3, return code 8 ( Label switched at stack-depth 1).` |
| `'P' - problem:` | A synchronization problem between the control and data planes was discovered at the designated LSR or at some transit LSR along the way.<br>Example<br>Suppose you have sent an MPLS echo packet to an LSR with an interface IP 100.2.1.3, and this LSR received the packet |

| LSP PING/Traceroute Reply | Significance |
|---|---|
| | with an MPLS label that *does not* match the label appearing in its MPLS ILM table. In such case, the LSR should return an MPLS Echo reply with return code 10, and the following line would appear on your screen:<br>`P     100.2.1.3, return code: 10 (Mapping for this FEC is not the given label at stack-depth 1)` |
| `'Q' - request not transmitted:` | The OS900 has no matching MPLS information in its control plane table to decide how to forward the packet.<br>Example<br>Suppose you try to send an MPLS PING message to FEC 4.4.4.4/32 using information learned via LDP and this FEC was either not learned via LDP or the OS900 is using RSVP for this FEC. In such case, you most likely will get the following reply:<br>`Q     Echo packet not sent to LDP ipv4 4.4.4.4/32 (check log file for explanation).` |
| `'U' - unreachable:` | No reply was received from the designated LSR (the egress LSR for the compatible FEC), or (when Traceroute is invoked) a transit LSR with a matching TTL did not reply. |

# LSP Traceroute

## General

LSP Traceroute functions like MPLS LSP PING. Like MPLS LSP PING, it enables the user to determine if an LSP can actually deliver user traffic.

The MPLS traceroute is designed to perform fault isolation, i.e., to detect the specific node in which the problem of synchronization between the control and data planes occurred. For this purpose, the MPLS echo packet is sent to the control plane of each transit LSR which then performs various checks to verify that it is indeed a transit LSR in the examined LSP.

Unlike the case of MPLS PING mentioned above, here, parameters in the MPLS echo packet IP header cannot be a trigger to send the packet to the control plane. This is of-course true since transit LSRs do not examine the packets' IP headers but only their MPLS headers. In order to trigger a transit OS900 to send the MPLS echo request packet to the control plane, the MPLS Traceroute command generates the MPLS echo packet with an increasing value of MPLS TTL (exactly like in regular IP-based traceroute). Each time an MPLS packet reaches an LSR with MPLS TTL 1, it causes the OS900 to send the packet to the control plane for further examination.

When MPLS PING has failed to verify end-to-end connectivity, it is advised to invoke the MPLS Traceroute command to pin-point the problematic LSR.

Again, the user cannot send traceroute packets over an RSVP LSP or LDP LSP that end at the same FEC at the same time. Moreover, the OS900 will not send echo packets over LDP LSP if for the same FEC an RSVP LSP exists.

## Over a Regular LDP LSP

To run LSP Traceroute over a regular LDP LSP:

1. Enter **enable** mode.
2. Invoke the command:

   **traceroute mpls ipv4 A.B.C.D/M [max-ttl <1-65535>] [timeout <1-10>]**

   where,

   **ipv4**: Over MPLS LDP-IPv4 tunnel.

   **A.B.C.D/M**: IPv4 host/network of the LDP FEC for which the MPLS echo packet is to be generated.

   **max-ttl**: Maximim time-to-live.

**<1-65535>**: Value for maximim time-to-live. Default: 30.
**timeout**: Set the maximum wait time between consecutive echo requests.
**<1-10>**: Time in seconds. Default: 1.

## Over an RSVP-TE LSP

To run LSP Traceroute over an RSVP-TE LSP:

1. Enter **enable** mode.
2. Invoke the command:

   **traceroute mpls traffic-eng trunkname TRUNKNAME [max-ttl] [timeout]**

   where,
   **traffic-eng**: over MPLS RSVP tunnel
   **trunkname**: Identify RSVP-TE destination by Trunk Name
   **TRUNKNAME**: RSVP-TE Trunk Name
   **max-ttl**: Maximim time-to-live.
   **<1-65535>**: Value for maximim time-to-live. Default: 30.
   **timeout**: Set the maximum wait time between consecutive echo requests.
   **<1-10>**: Time in seconds. Default: 1.

## Stopping

To stop an LSP Traceroute process:

1. Enter **enable** mode.
2. Invoke the command:

   **traceroute mpls stop**

## Replies

Refer to the section *Replies*, page *748*.

# Chapter 42: Provision

## General

This utility is used to provision Layer 2 Ethernet services and to control traffic flows in services in accordance with the Metro Ethernet Forum (MEF) specifications. To provision a service, it must first be configured and then enabled. To control a traffic flow, it must be classified and one or more actions to be performed on it must be selected. To facilitate configuration of services and classification of flows, profiles can be created and then incorporated in the service configuration or flow classification.

## Services

### Basic Configuration

To configure an Ethernet service, enter the provision mode as follows:

1 Enter **`configure terminal`** mode.

2 Enter provision mode by invoking the command:
  **`provision`**

3 Name the Ethernet service (and enter its mode) by invoking the command:
  **`service SERVICE_NAME`**
  where,
  **`SERVICE_NAME`**: Alphanumeric string without blanks.
  (To delete the service name (and service), invoke the command **`no service SERVICE_NAME`**.)

4 Select the service type by invoking the command:
  **`type (epl|evpl|ep-lan|evp-lan)`**
  where,
  **`epl`**: Ethernet Private Line Service.
  **`evpl`**: Ethernet Virtual Private Line Service.
  **`ep-lan`**: Ethernet Private LAN Service.
  **`evp-lan`**: Ethernet Virtual Private LAN Service.

5 Define the customer port(s) by invoking the command:
  **`c-ports PORTS-GROUP`**
  where,
  **`PORTS-GROUP`**: Group of customer ports.

6 Define the service port(s) by invoking the command:
  **`s-ports PORTS-GROUP`**
  where,
  **`PORTS-GROUP`**: Group of service ports.

7 Define the customer VLANs (applicable only for **`evpl`** and **`evp-lan`**) by invoking the command:
  **`c-vlans TAGS-LIST`**
  where,
  **`TAGS-LIST`**: Group of customer VLANs.

8 Define the service provider VLAN by invoking the command:
  **`s-vlan <1-4095>`**
  where,

**<1-4095>**: Service VLAN tag in the range 1 to 4095.

## Optional Configuration Parameters

### OAM

1 Include untagged packets by invoking the command:
**includes-untagged**
(To exclude untagged packets, invoke the command **no includes-untagged**.)

2 Enable transmission of CCMs by invoking the command:
**ccm enable**
(To disable transmission of CCMs, invoke the command **no ccm enable**.)

3 Define the Maintenance Association by invoking the command:
**oam ma NUMBER**
where,
**NUMBER**: Index of the Maintenance Association as a decimal number (in the range 1 to 65535) or hex number (in the range 0x0001 to 0xffff).
(To delete the Maintenance Association, invoke the command **no oam ma [NUMBER]**.)

4 Define the Maintenance Domain Level by invoking the command:
**oam md <0-7>**
where,
**NUMBER**: Level of the Maintenance Domain.
(To delete the Maintenance Domain Level, invoke the command **no oam md [NUMBER]**.)

5 Specify port of Maintenance Association End Point (MEP) by invoking the command:
**oam mep-port PORT**
where,
**PORT**: Port number. (The port can be a trunk. Trunks are described in ***Chapter 13:*** *IEEE 802.3ad Link Aggregation (LACP)*, page *273*.)
(To delete the MEP, invoke the command **no oam mep-port [PORT]**.)

6 Define the MEP identifier by invoking the command:
**oam mepid <1-4095>**
where,
**<1-4095>**: MEP identifier.
(To delete the MEP identifier, invoke the command **no oam mepid [NUMBER]**.)

7 Define the Performance Monitoring destination MAC address by invoking the command:
**pm destination mac MAC_ADDRESS**
where,
**MAC_ADDRESS**: MAC address in the hex format aa:bb:cc:dd:ee:ff.
(To delete the Performance Monitoring destination MAC address, invoke the command **no pm destination mac [MAC_ADDRESS]**.)

8 Specify the Performance Monitoring remote MEP identifier by invoking the command:
**pm destination rmep <1-4095>**
where,
**<1-4095>**: Remote MEP ID.
(To delete the remote MEP, invoke the command **no pm destination rmep [NUMBER]**.)

9 Define the Connectivity Fault Management (CFM) profile by invoking the command:
**cfm profile NAME**
where,
**NAME**: Name for CFM profile.
(To delete the CFM profile name, invoke the command **no cfm profile [NAME]**.)

10 Define the Performance Monitoring profile by invoking the command:
**pm profile NAME**

where,

**NAME**: Name of Performance Monitoring profile

(To delete the Performance Monitoring profile, invoke the command **no pm profile [NAME]**.)

11 Enable Performance Monitoring by invoking the command:

**pm enable**

(To disable Performance Monitoring, invoke the command **no pm enable**.)

12 Define the CoS for transmitted CCM packets by invoking the command:

**ccm cos <1-8>**

where,

**<1-8>**: CoS in the range 1 to 8.

(To set the CoS for transmitted CCM packets to the default value (**1**), invoke the command **no ccm cos [NUMBER]**.)

**QoS**

1 Select the service type by invoking the command:

**classify-flow-by (none|pcp|dscp)**

where,

**dscp**: Classification by DSCP.

**none**: Without classification.

**pcp**: Classification by Priority Code Point (PCP).

2 Define the Class of Service (CoS) for ingress packets that do not meet the flow conditions by invoking the command:

**mark pcp <0-7>**

where,

**<0-7>**: PCP in the range 0 to 7.

(To set the CoS for ingress packets to the default value (**1**), invoke the command **no default-cos [NUMBER]**.)

3 Enable ingress traffic bandwidth accounting by invoking the command:

**ingress-bw accounting**

(To disable ingress traffic bandwidth accounting, invoke the command **no ingress-bw accounting**.)

4 Assign an existing ingress traffic bandwidth profile to the service by invoking the command:

**ingress-bw profile NAME**

where,

**NAME**: Name for ingress traffic bandwidth profile.

(To remove the ingress traffic bandwidth profile, invoke the command **no ingress-bw profile [NAME]**.)

5 Enable egress traffic bandwidth accounting by invoking the command:

**egress-bw accounting**

(To disable egress traffic bandwidth accounting, invoke the command **no egress-bw accounting**.)

6 Assign an existing egress traffic bandwidth profile to the service by invoking the command:

**egress-bw profile NAME**

where,

**NAME**: Name for egress traffic bandwidth profile.

(To remove the egress traffic bandwidth profile, invoke the command **no egress-bw profile [NAME]**.)

**Layer 2 Protocol Tunneling**

Select the Layer 2 protocol tunneling mode by invoking the command:

**`l2protocol (cdp|efm|dot1x|esmc|lacp|pvst+|stp|vtp|udld) mode (drop|peer|transparent|tunnel)`**

where,

**`cdp`**: CISCO Discovery protocol

**`efm`**: Ethernet in the First Mile (IEEE 802.3ah) protocol

**`dot1x`**: Port-based network access control protocol

**`esmc`**: Ethernet Synchronization Messaging Channel protocol

**`lacp`**: Link-Aggregation Control protocol

**`pvst+`**: CISCO Per VLAN Spanning Tree protocol

**`stp`**: Spanning Tree protocol

**`vtp`**: CISCO VLAN Trunking protocol

**`udld`**: Unidirectional Link Detection protocol

**`drop`**: Discard packets

**`peer`**: Participate in the protocol

**`transparent`**: Transparent processing

**`tunnel`**: Tunnel with destination MAC replacement

(To revoke Layer 2 protocol tunneling of selected protocol, invoke the command **`no includes-untagged`**.)

#### Swapping Customer VLAN Tags

To enable swapping of the customer VLAN tag present in an egress packet to that of the customer tag of a VLAN at another UNI, invoke the command:

**`c-ing-tag-preserv <1-4095>`**

where,

**`<1-4095>`**: Customer tag of VLAN at another UNI.

(To revoke VLAN tag swapping, invoke the command **`no c-ing-tag-preserv [<1-4095>]`**.)

#### Binding an MTU Profile to a Service

To bind an MTU profile to a specific service, invoke the command:

**`mtu-profile <1-8>`**

where,

**`<1-8>`**: Number of profile.

(To unbind an MTU profile from a specific service, invoke the command **`no mtu-profile [NUMBER]`**.)

#### RFC2544

##### *Port*

To select the physical port for RFC2544 testing traffic, invoke the command:

**`rfc2544 transmit-port PORT`**

where,

**`PORT`**: Number of physical port for RFC2544 testing traffic.

(To cancel selection of the physical port for RFC2544 testing traffic, invoke the command **`no rfc2544 transmit-port [PORT]`**.)

##### *IP Address of Inband VLAN Interface*

To set the IP address of the Inband VLAN Interface for RFC2544 testing, invoke the command:

**`ip A.B.C.D/M`**

where,

**`A.B.C.D/M`**: IPv4 address and mask for Inband VLAN Interface.

(To cancel the IP address of the Inband VLAN Interface for RFC2544 testing, invoke the command **`no ip [A.B.C.D/M]`**.)

***Direction of Traffic to the FPGA***

To enable traffic received at Inband VLAN Interfaces to be directed to the FPGA for RFC2544 testing, invoke the command:

**`ip-sla`**

(To cancel direction of traffic to the FPGA, invoke the command **`no ip-sla`**.)

***Responder MAC Address***

To enter the MAC Address of the responder OS900 (at which frames are to be received) in RFC2544 testing, invoke the command:

**`responder-mac MAC_ADDRESS`**

where,

**`MAC_ADDRESS`**: MAC Address of the responder OS900.

(To cancel the MAC Address of the responder OS900, invoke the command **`no responder-mac [MAC_ADDRESS]`**.)

***Source MAC Address***

To enter the MAC Address of the Source OS900 for RFC2544 testing, invoke the command:

**`rfc2544 src-mac MAC_ADDRESS`**

where,

**`MAC_ADDRESS`**: MAC Address of the Source OS900.

(To cancel the MAC Address of the Source OS900, invoke the command **`no rfc2544 (src-mac [MAC_ADDRESS]`**.)

***Destination MAC Address***

To enter the MAC Address of the Destination OS900 for RFC2544 testing, invoke the command:

**`rfc2544 dest-mac MAC_ADDRESS`**

where,

**`MAC_ADDRESS`**: MAC Address of the Destination OS900.

(To cancel the MAC Address of the Destination OS900, invoke the command **`no rfc2544 dest-mac [MAC_ADDRESS]`**.)

***Destination IP Address***

To enter the IP Address or hostname of the Destination OS900 for RFC2544 testing, invoke the command:

**`rfc2544 dest-ip TARGET`**

where,

**`TARGET`**: IP Address or hostname of the Destination OS900.

(To cancel the IP Address or hostname of the Destination OS900, invoke the command **`no rfc2544 dest-ip [TARGET]`**.)

***Enabling***

To enable RFC2544 testing by the OS900, invoke the command:

**`rfc2544 enable`**

(To disable RFC2544 testing, invoke the command **`no rfc2544 enable`**.)

***Profile***

To create a profile for RFC2544 testing, invoke the command:

**`rfc2544 profile NAME`**

where,

**`NAME`**: Name of profile for RFC2544 testing.

(To cancel the profile, invoke the command **`no rfc2544 dest-ip [TARGET]`**.)

***ToS***

To assign the DiffServ ToS to RFC2544 testing, invoke the command:

**`rfc2544 tos <0-255>`**

where,

**`<0-255>`**: ToS for RFC2544 testing.
(To cancel the ToS assigned to RFC2544 testing, invoke the command **`no rfc2544 tos <0-255>`**.)

## Viewing

### Status of Services

To view the status of Ethernet services:

1. Enter **`provision`** mode.
2. Invoke the command:
   **`show services [detail]`**
   where,
   **`[detail]`**: In detail.

Alternatively, the status of Ethernet services can be viewed by entering **`enable`** mode and invoking the command: **`show ethernet services [detail]`**.

### Configurations of all Services

To view the *user* configurations of all Ethernet services:

1. Enter **`provision`** mode.
2. Invoke the command:
   **`show configuration`**

To view the *running* configurations of all Ethernet services:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show running-config provision`**

To view how provisioning commands are translated into *low-level commands*:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show provision service low-level-entities`**

### Configuration of a Specific Service

To view the configuration of a specific Ethernet service, *first* enter the mode of the service by invoking the command:

**`service SERVICE_NAME`**
where,
**`SERVICE_NAME`**: Name of the service whose configuration is to be viewed

#### *Service Ingress Counters*

To view ingress traffic bandwidth counter readings, invoke the command:

**`show ingress-bw [counters]`**
where,
**`[counters]`**: Not to be typed, serves as an indicator only!

These counter readings can also be viewed from **`enable`** mode by invoking the command:

**`show provision service SERVICE_NAME ingress-bw [counters]`**

#### *Service Egress Counters*

To view egress traffic bandwidth counter readings, invoke the command:

**`show egress-bw [counters]`**
where,
**`[counters]`**: Not to be typed, serves as an indicator only!

These counter readings can also be viewed from **`enable`** mode by invoking the command:

**`show provision service SERVICE_NAME egress-bw [counters]`**

***CCM Status***

To view the Continuity Check (CC) status for the service, invoke the command:

**`show ccm`**

***Remote MEPs***

To view CCM remote MEPs database, invoke the command:

**`show rmeps`**

***Current Configuration***

To view the current provision configuration of the service, invoke the command:

**`show configuration`**

***Performance Monitoring***

For performance monitoring, invoke the command:

**`show pm history|last-result`**

where,

**`history`**: History of results

**`last-result`**: Last result

***Running Configuration***

To view the running configuration of *a specific* Ethernet service:

1. Enter **`enable`** mode
2. Invoke the command:

   **`show running-config provision service SERVICE_NAME`**

   where,

   **`SERVICE_NAME`**: Name of the service whose configuration is to be viewed

***Low-level Commands***

To view how provisioning commands are translated into *low-level commands* for the service:

**`show low-level-commands`**

These *low-level commands* can also be viewed from **`enable`** mode by invoking the command:

**`show provision service low-level-entities NAME`**

where,

**`NAME`**: Name of the service whose low-level entities are to be viewed

## Activating

Before activating a service make sure that flows (if required) have been configured for the service.

To activate a service:

1. Enter **`provision`** mode.
2. Enter the mode of the service by invoking the command:

   **`service SERVICE_NAME`**

   where,

   **`SERVICE_NAME`**: Name of the service.
3. Invoke the command:

   **`enable`**

## Deactivating

To deactivate a service:

1. Enter **`provision`** mode.
2. Enter the mode of the service by invoking the command:

   **`service SERVICE_NAME`**

   where,

   **`SERVICE_NAME`**: Name of the service.

3. Invoke the command:
   **`no enable`**

## Clearing Statistics

To clear Ethernet OAM statistics counters for *the service*, invoke the command:
**`oam clear-statistics`**
To clear the ingress bandwidth counters for a service, invoke the command:
**`clear ingress-bw [counters]`**
where,
`[counters]`: Not to be typed, serves as an indicator only!
The ingress bandwidth counters can also be cleared from **`enable`** mode by invoking the command:
**`clear provision service SERVICE_NAME ingress-bw [counters]`**
To clear the egress bandwidth counters for a service, invoke the command:
**`clear egress-bw [counters]`**
where,
`[counters]`: Not to be typed, serves as an indicator only!
The egress bandwidth counters can also be cleared from **`enable`** mode by invoking the command:
**`clear provision service SERVICE_NAME egress-bw [counters]`**

## Deleting

To delete a service:
1. Enter **`provision`** mode.
2. Invoke the command:
   **`no service SERVICE_NAME`**
   where,
   **`SERVICE_NAME`**: Name of service.

# Flows

Flows represent different service levels or classes of service (CoS) for services. Each flow can be remarked, rate limited (policed), and monitored separately.
To configure a flow, first enter the mode of a service level (by invoking the command **`service SERVICE_NAME`** from **`provision`** mode).

## Basic Configuration

### Classification

1 Name the flow by assigning a CoS value to it using the command:
**`flow <1-8>`**
where,
**`<1-8>`**: CoS of the flow.
(To delete the flow, invoke the command **`no flow <1-8>`**)
2 Create an Ethernet OAM MEP identifier by invoking the command:
**`oam mepid <1-4095>`**
where,
**`<1-4095>`**: Maintenance Association End Point identifier.
(To delete an Ethernet OAM MEP identifier, invoke the command **`no oam mepid [NUMBER]`**.)
3 Define the Performance Monitoring destination MAC address by invoking the command:
**`pm destination mac MAC_ADDRESS`**

where,

**MAC_ADDRESS**: MAC address in the hex format aa:bb:cc:dd:ee:ff.

(To delete the Performance Monitoring destination MAC address, invoke the command **no pm destination mac [MAC_ADDRESS]**.)

4 Specify the Performance Monitoring remote MEP identifier by invoking the command:

**pm destination rmep <1-4095>**

where,

**<1-4095>**: Remote MEP ID.

(To delete the remote MEP, invoke the command **no pm destination rmep [NUMBER]**.)

5 Select the VLAN tag for the CoS value by invoking the command:

**tag <1-4094>**

where,

**<1-4095>**: VLAN tag in the range 1 to 4095.

(To remove the assignment, invoke the command **no tag <1-4094>**.)

6 Define the Performance Monitoring profile by invoking the command:

**pm profile NAME**

where,

**NAME**: Name of Performance Monitoring profile

(To delete the Performance Monitoring profile, invoke the command **no pm profile [NAME]**.)

7 Enable Performance Monitoring by invoking the command:

**pm enable**

(To disable Performance Monitoring, invoke the command **no pm enable**.)

8 Assign the default CoS to the DSCP value by invoking the command:

**dscp DSCP_VALUE**

where,

**DSCP_VALUE**: DSCP value of ingress packets in the range decimal [0 - 63] or hex [0x0 - 0x3f].

(To remove the assignment, invoke the command **no dscp DSCP_VALUE**.)

9 Assign the default CoS to the PCP value by invoking the command:

**pcp <0-7>**

where,

**<0-7>**: PCP value of ingress packets in the range decimal [0 to 7].

(To remove the assignment, invoke the command **no pcp <0-7>**.)

### Actions

1 Enable ingress traffic bandwidth accounting by invoking the command:

**ingress-bw accounting**

(To disable ingress traffic bandwidth accounting, invoke the command **no ingress-bw accounting**.)

2 Assign an existing ingress traffic bandwidth profile to the service by invoking the command:

**ingress-bw profile NAME**

where,

**NAME**: Name for ingress traffic bandwidth profile.

(To remove the ingress traffic bandwidth profile, invoke the command **no ingress-bw profile [NAME]**.)

3 Enable egress traffic bandwidth accounting by invoking the command:

**egress-bw accounting**

(To disable egress traffic bandwidth accounting, invoke the command **no egress-bw accounting**.)

4 Assign an existing egress traffic bandwidth profile to the service by invoking the command:

**`egress-bw profile NAME`**

where,

**`NAME`**: Name for egress traffic bandwidth profile.

(To remove the egress traffic bandwidth profile, invoke the command **`no egress-bw profile [NAME]`**.)

5 Mark *egress* packets with a new DSCP and/or PCP according to the SL of the packet using a global map (described in the section *Marking*, page *285*, in ***Chapter 14:*** *Quality of Service (QoS)*) by invoking the command:

**`mark dscp <0-63>`**

where,

**`<0-63>`**: DSCP value of ingress packets in the range decimal [0 to 63] or hex [0x0 to 0x3f].

(To disable DSCP marking, invoke the command **`no mark dscp [NUMBER]`**.)

Or

**`mark pcp <0-7>`**

where,

**`<0-7>`**: PCP value of ingress packets in the range decimal [0 to 7].

(To disable PCP marking, invoke the command **`no mark pcp [NUMBER]`**.)

6 Assign the bandwidth profile to packets in flows that do not have DSCP priority bits (such as non-IP packets) by invoking the command:

**`rest-of-traffic`**

## Viewing

To view the flow of an Ethernet service, first enter the mode of the flow by invoking the commands:

**`service SERVICE_NAME`**

where,

**`SERVICE_NAME`**: Name of the service whose configuration is to be viewed

and

**`flow <1-8>`**

where,

**`<1-8>`**: CoS of the flow.

### *Ingress Traffic Bandwidth*

To view ingress traffic bandwidth counter readings, invoke the command:

**`show ingress-bw [counters]`**

where,

`[counters]`: Not to be typed, serves as an indicator only!

These counter readings can also be viewed from **`enable`** mode by invoking the command:

**`show provision service SERVICE_NAME flow <1-8> ingress-bw [counters]`**

### *Egress Traffic Bandwidth*

To view egress traffic bandwidth counter readings, invoke the command:

**`show egress-bw [counters]`**

where,

`[counters]`: Not to be typed, serves as an indicator only!

These counter readings can also be viewed from **`enable`** mode by invoking the command:

**`show provision service SERVICE_NAME flow <1-8> ingress-bw [counters]`**

### *Current Configuration*

To view the current Ethernet OAM configuration of the OS900, invoke the command:

**`show configuration`**

***Low-level Commands***

To view low-level commands, invoke the command:

**`show low-level-commands`**

***Performance Monitoring***

For performance monitoring, invoke the command:

**`show pm history|last-result`**

where,

**`history`**: History of results

**`last-result`**: Last result

## Clearing Statistics

To clear Ethernet OAM statistics counters for *the flow*, invoke the command:

**`oam clear-statistics`**

To clear the ingress bandwidth counters for a flow, invoke the command:

**`clear ingress-bw [counters]`**

where,

**`[counters]`**: Not to be typed, serves as an indicator only!

The ingress bandwidth counters can also be cleared from **`enable`** mode by invoking the command:

**`clear provision service SERVICE_NAME flow <1-8> ingress-bw [counters]`**

To clear the egress bandwidth counters for a flow, invoke the command:

**`clear egress-bw [counters]`**

where,

**`[counters]`**: Not to be typed, serves as an indicator only!

The egress bandwidth counters can also be cleared from **`enable`** mode by invoking the command:

**`clear provision service SERVICE_NAME flow <1-8> egress-bw [counters]`**

## Deleting

To delete a flow, invoke the command:

**`no flow <1-8>`**

where,

**`<1-8>`**: CoS of the flow.

# Profiles

The following three types of profile can be configured:

– Bandwidth Provisioning Profile
– Connectivity Fault Management Profile
– Performance Monitoring Profile

A profile can be assigned to Flows and Ethernet Services.

## Bandwidth Provisioning Profile

### Configuration

To create a Bandwidth profile for traffic (for details refer to ***Chapter 19:*** *Traffic* Conditioner, page *357*):

1. Enter **`provision`** mode.
2. Create a profile by invoking the command:

   **`bw profile NAME`**

where,

**NAME**: Bandwidth profile name.

(To delete the Bandwidth profile, invoke the command **no bw profile NAME**.)

3. Set the Committed Burst Size (CBS) by invoking the command:

   **cbs BURSTSIZE**

   where,

   **BURSTSIZE**: CBS value. The value may be any number in the range 4K-16M bytes (in units K, M). Valid units are: k, m. (Examples: **7k**, **2m**.). It is recommended to select a value that is at least as large as the largest possible packet in the stream. If the value **0** is selected, all packet flows to which this profile is assigned will be marked with the traffic conditioner CL 'red.'

   (To reset the CBS to the default value, i.e., **0**, invoke the command **no cbs BURSTSIZE**.)

4. Set the Committed Information Rate (CIR) by invoking the command:

   **cir RATELIMIT**

   where,

   **RATELIMIT**: CIR value. Valid units are: k, m, g. (Examples: **100k**, **10m**., **1g**). If the value **0** is selected, all packet flows to which this profile is assigned will be marked with the traffic conditioner CL 'red.'

   (To allow any CIR rate, invoke the command **no cir [RATELIMIT]**.)

5. Select the mode for handling colored packets by invoking the command:

   **color-mode (blind|aware|drop-red)**

   where,

   **aware**: Color-aware mode, i.e., colors to be distinguished.

   **blind**: Blind mode, i.e., colors to be ignored. Default mode.

   **drop-red**: Color-aware mode + Policing, i.e., colors to be distinguished and red packets to be discarded.

   (To set handling of packets according to the default mode (**blind**), invoke the command **no color-mode [MODE]**, where **[MODE]** can be **aware**, **blind**, **drop-red**.)

6. (Applicable only to OS9124-410G) Set the Excess Burst Size (EBS) by invoking the command:

   **ebs BURSTSIZE**

   where,

   **BURSTSIZE**: EBS value. Valid units are: k, m. (Examples: **7k**, **2m**.).

   (To reset the EBS to the default value, i.e., **0**, invoke the command **no ebs [BURSTSIZE]**.)

7. (Applicable only to OS9124-410G) Set the Excess Information Rate (EIR) by invoking the command:

   **eir RATELIMIT**

   where,

   **RATELIMIT**: EIR value. Valid units are: k, m, g. (Examples: **100k**, **10m**., **1g**).

   (To allow any EIR rate, invoke the command **no eir [RATELIMIT]**.)

### Viewing

To view the current configuration of the node or enabled services/flows that use this Bandwidth profile:

1. Enter **provision** mode.
2. Enter the mode of the specific profile by invoking the command:

   **bw profile NAME**

   where,

   **NAME**: Bandwidth profile name.

3. To view the current configuration of the node, invoke the command:

   **show configuration**

To view enabled services/flows, invoke the command:

**`show active-owners`**

### Deleting

To delete a Bandwidth profile:

1. Enter **`provision`** mode.
2. Invoke the command:

   **`no bw profile NAME`**

   where,

   **`NAME`**: Bandwidth profile name

## Connectivity Fault Management Profile

### Configuration

To create a Connectivity Fault Management profile for traffic:

1 Enter **`provision`** mode.

2 Create a profile by invoking the command:

   **`cfm profile NAME`**

   where,

   **`NAME`**: Connectivity Fault Management profile name

   (To delete the Connectivity Fault Management profile, invoke the command **`no cfm profile NAME`**.)

3 Set the time interval between CCM PDUs sent by MEPs by invoking the command:

   **`ccm-interval (100ms|10ms|10s|1s|300Hz|600s|60s|none)`**

   where,

   **`100ms`**: 100 millisecond

   **`10ms`**: 10 millisecond

   **`10s`**: 10 seconds

   **`1s`**: 1 second - default

   **`300Hz`**: 3 1/3 millisecond

   **`600s`**: 10 minutes

   **`60s`**: 1 minute

   **`none`**: MEPs will not send CCMs

   **`INTERVAL`**: Time interval between CCM PDUs

   (To reset time interval to the default (**`1s`**), invoke the command **`no ccm-interval [INTERVAL]`**.)

4 Set the time that defects must be *present* before a CCM Fault Alarm is issued by invoking the command:

   **`fng-alarm-time <250-1000>`**

   where,

   **`<250-1000>`**: Value of time in the range 250 to 1000 ms. The value must be a multiple of 10.

   (To reset the time to the default (**`2.5`** seconds) , invoke the command **`no fng-alarm-time`**.)

5 Set the time defects must be *absent* before a CCM Fault Alarm is disabled by invoking the command:

   **`fng-reset-time <250-1000>`**

   where,

   **`<250-1000>`**: Value of time in the range 250 to 1000 ms. The value must be a multiple of 10.

(To reset the time to the default (**10** seconds) , invoke the command **no fng-reset-time**.)

6 Set the lowest CCM defect priority that will issue an alarm by invoking the command:

**lowest-alarm-prio (all|error|mac_status|none|rdi|rmep)**

where,

**all**: All defects: RDI, MACStatus, Remote MEPs fault, ErrorCCM, XCON CCM

**error**: ErrorCCM and above: XCON

**mac_status**: MACStatus and above: Remote MEPs fault, ErrorCCM, XCON CCM

**none**: Nothing to inform

**rdi**: RDI and above: MACStatus, Remote MEPs fault, ErrorCCM, XCON CCM - default

**rmep**: Remote MEPs fault and above: ErrorCCM, XCON CCM

(To reset the CCM defect priority to the default (**rdi**), invoke the command **no lowest-alarm-prio (all|error|mac_status|none|rdi|rmep)**.)

### Viewing

To view the current configuration of the node:

1. Enter **provision** mode.
2. Enter the mode of the specific profile by invoking the command:

   **cfm profile NAME**

   where,

   **NAME**: Connectivity Fault Management profile name
3. Invoke the command:

   **show configuration**

### Deleting

To delete a Connectivity Fault Management profile:

1. Enter **provision** mode
2. Invoke the command:

   **no cfm profile NAME**

   where,

   **NAME**: Connectivity Fault Management profile name

## Performance Monitoring Profile

### Configuration

To create a Performance Monitoring profile for traffic:

1. Enter **provision** mode.
2. Create a profile by invoking the command:

   **pm profile NAME**

   where,

   **NAME**: Performance Monitoring profile name

   (To delete the Performance Monitoring profile, invoke the command **no pm profile NAME**.)
3. Limit the number of most recent history entries by invoking the command:

   **history-size <2-65535>**

   where,

   **<2-65535>**: Number of history entries (default 5)

   (To reset the limit to the default (**5**), invoke the command **no history-size [NUMBER]**.)

4. Set the time interval between every two packets in a burst by invoking the command:
   **`interval <1-1000000> [msec|usec]`**
   where,
   **`<1-1000000>`**: Interval between packets in ms or µs

   (To reset the time interval to the default (**`100 ms`**), invoke the command **`no interval [NUMBER]`**.)
5. Set the time interval between every two bursts by invoking the command:
   **`interval-between-bursts <1-86400>`**
   where,
   **`<1-86400>`**: Interval between bursts in seconds.

   (To reset the time interval to the default (**`60`** seconds), invoke the command **`no interval-between-bursts [NUMBER]`**.)
6. Set the PDU length (measured in the Layer 2 header up to and excluding CRC) that will help diagnose faults sensitive to this length by invoking the command:
   **`length <60-9000>`**
   where,
   **`<60-9000>`**: Bytes (default 60)

   (To reset the length to the default (**`60`**), invoke the command **`no length [NUMBER]`**.)
7. Set the number of frame transmission bursts by invoking the command:
   **`number-of-bursts (unlimited|<1-255>)`**
   where,
   **`<1-255>`**: Number of bursts
   **`unlimited`**: Continual transmission

   (To reset the number of bursts to the default (**`1`**), invoke the command **`no number-of-bursts [NUMBER]`**.)
8. Set the number of packets to be sent during each burst interval by invoking the command:
   **`packets-in-burst <1-1000000>`**
   where,
   **`<1-1000000>`**: Number of packets to be sent in one burst (default 3)

   (To reset the number to the default (**`3`**), invoke the command **`no packets-in-burst [NUMBER]`**.)
9. Set a data pattern (inside a PDU) that will help to diagnose faults sensitive to incompleteness of data in a frame by invoking the command:
   **`pattern HEXLINE`**
   where,
   **`HEXLINE`**: Hexadecimal pattern, for example, 0f0f0a0a

   (To reset the pattern to the default (**`DataFill`**), invoke the command **`no pattern [HEXLINE]`**.)
10. Set the Performance Monitoring frame-delay or jitter thresholds for averages in a burst that will cause alarms to be sent to the CLI or SNMP manager when crossed by invoking the command:
    **`threshold (frame-delay|ds-jitter|sd-jitter) rise <0-10000000> fall <0-10000000>`**
    where,
    **`frame-delay`**: Frame delay
    **`ds-jitter`**: Destination-Source jitter
    **`sd-jitter`**: Source-Destination jitter
    **`rise`**: Rise threshold
    **`<0-10000000>`**: Rise threshold value (microseconds)
    **`fall`**: Fall threshold

**<0-10000000>**: Fall threshold value (microseconds)

11. Set the maximum time the Delay-Measurement/Loopback mechanism is to wait for a response to its request PDU by invoking the command:
    **timeout <1-60000>**
    where,
    **<1-60000>** Timeout in milliseconds (default 200)

    (To reset the wait time to the default (**200**), invoke the command **no timeout <1-60000>**.)
12. Set the test type by invoking the command:
    **type (dmm|lbm) [slow]**
    where,
    **dmm**: Frame Delay Measurement (default)
    **lbm**: Ethernet Loopback
    **[slow]** : 'Slow' mode

    (To reset the test type to the default (**dmm**), invoke the command **no type [dmm|lbm]**.)

### Viewing

To view the current configuration of the node:

1. Enter **provision** mode.
2. Enter the mode of the specific profile by invoking the command:
   **pm profile NAME**
   where,
   **NAME**: Performance Monitoring profile name
3. Invoke the command:
   **show configuration**

### Deleting

To delete a Performance Monitoring profile:

1. Enter **provision** mode
2. Invoke the command:
   **no pm profile NAME**
   where,
   **NAME**: Performance Monitoring profile name

## RFC2544 Profile

### Configuration

To create an RFC 2544 profile for traffic:

1. Enter **provision** mode.
2. Create a profile by invoking the command:
   **rfc2544 profile NAME**

   (To delete  the profile, invoke the command: **no rfc2544 profile NAME**.)
3. Set the time (in seconds) during which the test is to run:
   **duration <1-3600>**

   where,
   **<1-3600>**: Test duration in seconds. Default: **0**, i.e., the number of packets per burst (as set with the command **packets-in-burst <1-1000000>**) is to be used instead of this parameter value.

   (To reset the time interval to the default value (**0**), invoke the command: **no duration**.)
4. Limit the number of most recent history entries by invoking the command:
   **history-size <2-65535>**

where,

**<2-65535>**: Number of history entries (default 5)

(To reset the number of history entries to the default value (5), invoke the command: **no history-size**.)

5. Set the time interval between traffic bursts by invoking the command:

   **interval-between-bursts <1-86400>**

   where,

   **<1-86400>**: Time interval (in seconds)

   (To reset the time interval between traffic bursts to the default value (60), invoke the command: **no interval-between-bursts [NUMBER]**.)

6. Set the time interval between packets by invoking the command:

   **interval-between-packets <1-1000000>**

   where,

   **<1-1000000>**: Interval (in microseconds)

   (To reset the time interval between packets to the default value (100000), invoke the command: **no interval-between-packets [NUMBER]**.)

7. Set the packet length (includes VLAN ID, L2VPT [802.1p] field bits, and CRC) for a test that will help diagnose faults sensitive to this length by invoking the command:

   **length <64-9216>**

   where,

   **<64-9216>**: Packet length (in bytes)

   (To reset the packet length to the default value (68), invoke the command: **no length [NUMBER]**.)

8. (This configuration parameter applies only for the *throughput test* type.)
   Set the maximum permitted % loss acceptable in determining the maximum datastream rate for such a loss by invoking the command:

   **loss-ratio <0-10000>**

   where,

   **<0-10000>**: Allowed loss in 0.01%. Default: 0 (0 %).

   (To reset the acceptable loss to the default value (0), invoke the command: **no loss-ratio**.)

9. Set the number of times a burst is to be performed by invoking the command:

   **number-of-bursts <1-4294967295>|unlimited**

   where,

   **<1-4294967295>**: Number of bursts (in decimal format).

   **unlimited**: Continual transmission.

   (To reset the number of times a burst is to be performed to the default value (1), invoke the command: **no number-of-bursts [NUMBER]**.)

10. Set the number of packets to be sent in one burst by invoking the command:

    **packets-in-burst <1-1000000>**

    where,

    **<1-1000000>**: Number of packets per burst).

    (To reset the number of packets to be sent in one burst to the default value (3), invoke the command: **no number-of-bursts [NUMBER]**.)

11. Add a data pattern (inside a packet) that will help to diagnose faults sensitive to incompleteness of data in a packet for a test by invoking the command:

    **pattern HEXLINE**

    where,

    **HEXLINE**: Pattern (dataFill) of DataTLV using hexadecimal digits, e.g., **0123fa9c**. The number of characters must be an integral multiple of 8.

(To reset the pattern to the default (**DataFill**), invoke the command **no pattern [HEXLINE]**.)

12. Select protocol for RFC 2544 testing by invoking the command:

    **protocol (dmmY1731|icmpEcho)**

    where,

    **dmmY1731**: Delay Measurement per the ITU-T Y.1731 standard.

    **icmpEcho**: ICMP echo per RFC 792.

    (To cancel the protocol for RFC 2544 testing, invoke the command **no protocol [dmmY1731|icmpEcho]**.)

13. Select the rate of the data stream by invoking the command:

    **rate RATELIMIT**

    where,

    **RATELIMIT**: Rate (in units of bits/sec). Any of the following multiples may be used in expressing the rate: **k** (= $10^3$), **m** (= $10^6$), or **g** (= $10^9$). Examples of valid rates: **5k**, **8m**, **1g**.

    (To set the rate to zero (and therefore prevent running of the test) invoke the command **no rate**.)

14. Select the an increment whose multiples will be used to adjust the datastream rate each time before running the test in order to determine the maximum rate for which the packet loss is less than the selected % described in the section *Percentage Loss*, page *491*:test by invoking the command:

    **step STEP**

    where,

    **STEP**: Increment size. Default: **1m** (1 Mbps).

    (To set the increment to the default value (**1m**), invoke the command: **no step**.)

15. Set the different packet lengths (each includes VLAN ID, L2VPT [802.1p] field bits, and CRC) for testing by invoking the command:

    **test-frame-lengths ..**

    where,

    **..**: Sequence of packet lengths. The lengths must be separated by blanks. Example: **test-frame-lengths 64 81 207**

    (To cancel the user-set packet lengths, invoke the command: **no test-frame-lengths ..**. If the argument **..** is excluded, all packet lengths will be canceled)

16. Set the Performance Monitoring frame-delay or jitter thresholds for averages in a burst that will cause alarms to be sent to the CLI or SNMP manager when crossed by invoking the command:

    **threshold (frame-delay|ds-jitter|sd-jitter) rise <0-10000000> fall <0-10000000>**

    where,

    **frame-delay**: Frame delay

    **ds-jitter**: Destination-Source jitter

    **sd-jitter**: Source-Destination jitter

    **rise**: Rise threshold

    **<0-10000000>**: Rise threshold value (microseconds)

    **fall**: Fall threshold

    **<0-10000000>**: Fall threshold value (microseconds)

    (To cancel alarm sending, invoke the command: **no threshold (frame-delay|ds-jitter|sd-jitter) [rise] [NUMBER] [fall] [NUMBER]**. If the argument **..** is excluded, all packet lengths will be canceled)

17. Set the maximum wait time for test completion by invoking the command:

    **timeout <1-60000>**

where,

**<1-60000>**: Wait time (in milliseconds) from the range 0 to 60000. Default: **200**.

18. Generate trap notification by invoking the command:

    **trap (all|burst-complete|burst-fail|test-complete|rtt|jitter|pcktLoss)**

    where,

    **burst-complete**: Generate osRfc2544BurstComplete trap notification.

    **burst-fail**: Generate osRfc2544BurstFail trap notification.

    **jitter**: Generate trap notification when osRfc2544ResultsJittAverage threshold is crossed.

    **pcktLoss**: Generate trap notification when osRfc2544ResultsPcktLoss threshold is crossed.

    **rtt**: Generate trap notification when osRfc2544ResultsRttAverage threshold is crossed.

    **test-complete**: Generate osRfc2544TestComplete trap notification.

    **all**: Generate all of the above trap notifications.

19. Set the time-to-live for IP packets by invoking the command:

    **ttl <1-255>**

    where,

    **<1-255>**: Time-to-live for IP packets from the range 1 to 255. Default: **128**.

20. Select the type of RFC 2544 test by invoking the command:

    **type basic|throughput|latency|frameLossRate**

    where,

    **basic**: Basic test.

    **throughput**: Throughput test.

    **latency**: Latency test.

    **frameLossRate**: Frame Loss Rate test.

**Viewing**

1. Enter **provision** mode.
2. Enter the mode of the specific profile by invoking the command:

    **rfc2544 profile NAME**

    where,

    **NAME**: RFC 2544 profile name

3. Invoke the command:

    **show configuration**

**Deleting**

To delete an RFC 2544 profile:

1. Enter **provision** mode
2. Invoke the command:

    **no rfc2544 profile NAME**

    where,

    **NAME**: RFC 2544 profile name

# Appendix A: Utilities

## General

This chapter describes and shows how to use the various network utilities of the OS900, which are:

- Domain Name System/Server (DNS)
- Traceroute
- TCP dump (built-in LAN analyzer)
- TELNET
- Secure Shell (SSH)
- Address Resolution Protocol (ARP)
- Configuration File Management
- Memory Management
- Multicast Destination MAC Addresses
- Debug Information
- Linux Tasks
- UniDirectional Link Detection Protocol

## MPLS and Routing Performance

### Viewing

To view statistical information on a protocol’s pseudo-threads (average time of run, maximum time of run, number of times the thread was called, etc.):

1. Enter **enable** mode
2. Invoke the command:

   **show thread cpu (nsm|ospf|isis|rip|bgp|ldp|rsvp) [FILTER]**

   where,

   **nsm**: MRV internal CPU process for managing routing protocols and MPLS
   **ospf**: OSPF process
   **isis**: ISIS process
   **rip**: RIP process
   **bgp**: BGP process
   **ldp**: LDP/RSVP process

### Clearing

To clear statistical information on a protocol’s pseudo-threads:

1. Enter **enable** mode
2. Invoke the command:

   **clear thread cpu (nsm|ospf|isis|rip|bgp|ldp|rsvp)**

   where,

   **nsm**: MRV internal CPU process for managing routing protocols and MPLS
   **ospf**: OSPF process
   **isis**: ISIS process

**rip**: RIP process
**bgp**: BGP process
**ldp**: LDP/RSVP process

# PING

## General

PING is a tool for determining whether a particular host is reachable across an IP network. It works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. In addition, PING measures the round-trip time and records any packet loss.

## Usage

To run PING:

1. Enter **enable** mode
2. Invoke any of the following commands:

**ping WORD**
**ping WORD count COUNT rate (RATE|rapid)**
**ping WORD count COUNT rate (RATE|rapid) size SIZE**
**ping WORD count COUNT rate (RATE|rapid) size SIZE source SOURCE**
**ping WORD count COUNT rate (RATE|rapid) size SIZE source SOURCE tos <0-254>**
**ping WORD count COUNT rate (RATE|rapid) source SOURCE**
**ping WORD count COUNT size SIZE**
**ping WORD count COUNT size SIZE source SOURCE**
**ping WORD count COUNT source SOURCE**
**ping WORD rate (RATE|rapid)**
**ping WORD rate (RATE|rapid) size SIZE**
**ping WORD rate (RATE|rapid) size SIZE source SOURCE**
**ping WORD rate (RATE|rapid) source SOURCE**
**ping WORD size SIZE**
**ping WORD size SIZE source SOURCE**
**ping WORD source SOURCE**

where,

**WORD**: Target/destination IP address or hostname.
**COUNT**: Number of PING requests to send.
(For an unlimited number, enter **0**).
**RATE**: Rate at which packets are to be sent, e.g., 2 or 0.1 (in packets/sec).
**rapid**: Shortest inter-packet interval conforming to round-trip time.
**SIZE**: Size of ICMP data (integer).
**SOURCE**: IP Address of source for specified interface or device name (alphanumeric string).
**<0-254>**: ToS value in the range **0** to **254**.
**SOURCE**: IP Address of source for specified interface or device name.

<u>Example</u>

```
OS910# ping 192.168.4.3
PING 192.168.4.3 (192.168.4.3) 56(84) bytes of data.
64 bytes from 192.168.4.3: icmp_seq=1 ttl=64 time=10.6 ms
64 bytes from 192.168.4.3: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.4.3: icmp_seq=3 ttl=64 time=0.324 ms
64 bytes from 192.168.4.3: icmp_seq=4 ttl=64 time=0.326 ms
64 bytes from 192.168.4.3: icmp_seq=5 ttl=64 time=0.988 ms

--- 192.168.4.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
```

```
rtt min/avg/max/mdev = 0.317/2.523/10.664/4.078 ms
OS910#
```

# Domain Name System/Server (DNS)

## General

A DNS is used in the Internet for translating hostnames (names of network nodes) into IP addresses, and vice versa. Its purpose is to allow system administrators to define nodes using mnemonics (rather than IP addresses), which are much more convenient for identifying nodes. The OS900 has a DNS client based on RFC 1591.

## Configuration

To configure the OS900 to operate with a DNS:

1. To define a domain name, invoke the command:

   **`domain-name NAME`**

   where,

   **`NAME`**: Your company's domain name. It identifies one or more hostnames. An example of a domain name is *mrv.com*. An example of a hostname belonging to this domain is *torro.mrv.com*. In URLs, domain names are used to identify particular Web pages. For example, in the URL *http://www.faqs.org/rfcs/rfc1213.html*, the domain name is *faqs.org*. Every domain name has a suffix that indicates the Top-Level Domain (TLD) to which it belongs. In the examples above, the domain name suffixes are *com* and *org*.
2. To define the IP address of the DNS (i.e., the server which is to translate the domain name into the IP addresses), invoke the command:

   **`nameserver A.B.C.D`**

   where,

   **`A.B.C.D`**: is the IP address of the DNS.
3. To enable DNS lookup services, invoke the command:

   **`enable`**

To view the configuration, invoke the command **`write terminal`** or **`write memory`**.

<u>Example</u>

```
OS900(config)# write terminal
Building configuration...

Current configuration:
! version 1_0_11
!
dns
 domain-name mrv.com
 nameserver 195.208.93.67
 enable
```

## Querying

To query the DNS regarding a hostname or IP address belonging to the name domain, invoke the command

**`nslookup HOST-TO-FIND`**

where,

**`HOST-TO-FIND`**: is hostname or IP address belonging to the name domain.

## Deleting

To delete the domain name, invoke the command

**`no domain-name`**

To disable DNS lookup services, invoke the command

**`no enable`**

To delete the domain nameserver, invoke the command

**`no nameserver A.B.C.D`**

where,

**`A.B.C.D`**: is the IP address of the DNS, i.e., the server which is to translate the domain name into the IP addresses.

# Traceroute

## Definition

Traceroute is a utility that traces the path of a packet sent from the OS900 to a host on the network, showing how many hops the packet requires in order to reach the host and how long each hop takes.

## Purpose

Traceroute can be used to determine, for example, where the longest delays occur. It can be used with IP SLA and VCD in isolating the source of a connectivity problem.

## Range

The OS900 can be used to trace a destination that is up to 30 hops away.

## Principle of Operation

The principle of Traceroute is as follows: Initially, it sends a packet with a very small Time-To-Live (TTL) field value. A TTL value specifies how many hops the packet is allowed before it is returned. When a packet cannot reach its destination due to the very small TTL value, the last host to receive the packet returns the packet and identifies itself.

By sending a series of packets, each having a successively higher TTL value, all the intermediary hosts can be identified.

Each traceroute packet is 40 bytes long. Three packets are sent to each of the hops on the way to the destination and there return time is measured.

## Usage

To perform traceroute:

1. Enter **`disable`** mode.
2. Invoke the command:

   **`traceroute`**: **`WORD`**

   where,

   **`WORD`**: IP address or DNS name of the destination host.

## Example

The following example shows the nine hops to the destination, the IP address of each hop, and the three return times for each hop.

```
OS900> traceroute 212.143.162.198
traceroute to 212.143.162.198 (212.143.162.198), 30 hops max, 40 byte packets
1 Zorro.gallant.co.il (10.90.131.254) 3.896 ms 3.167 ms 6.423 ms
2 router.gallant.co.il (10.90.134.254) 2.34 ms 2.393 ms 2.349 ms
3 10.90.138.233 (10.90.134.233) 2.348 ms 2.315 ms 2.31 ms
4 10.90.138.225 (10.90.134.225) 2.573 ms 2.375 ms 2.424 ms
5 tunnel-optic.ser.netvision.net.il (207.232.58.134) 4.571 ms 4.658 ms 3.953 ms
6 gi10-0.core1.hfa.nv.net.il (212.143.8.69) 128.406 ms 190.186 ms 199.244 ms
7 ge1-2.core1.pt.nv.net.il (212.143.12.66) 7.425 ms 6.301 ms 6.397 ms
8 g1-2.agr02.pt.nv.net.il (212.143.10.78) 6.638 ms 6.909 ms 6.429 ms
```

```
9 akm-tlv-198.netvision.net.il (212.143.162.198) 9.901 ms 7.179 ms 6.203 ms
OS900>
```

# TCP Dump

## Definition

TCP dump is display of the current traffic to the CPU via a specific interface.

## Purpose

TCP dump is used to troubleshoot network applications that communicate with the OS900.

## Usage

To perform TCP dump:

1. Enter **enable** mode.
2. Invoke the command:

   **tcpdump INTERFACE**

   where,

   **INTERFACE**: Interface via which traffic flows to the CPU. The interface must have the format **vifX**, where **X** is any number in the range 0-4095.

## Example

The example below shows:

Invocation of TCP dump using the command tcpdump vif90.

TCP dump (packet time, IP address, protocol port/number, captured packets, etc.)

Example

```
OS900# tcpdump vif90

23:51:34.108532 IP 192.83.205.242.telnet > 192.83.137.239.1041: P 2323:2775(452)
 ack 0 win 5840
23:51:34.293674 arp who-has 192.168.30.32 (Broadcast) tell 192.168.30.32
23:51:34.294664 IP 192.83.205.242.1027 > zot.tiger.co.il.domain:  19255+ PTR? 32
.30.168.192.in-addr.arpa. (44)
23:51:34.296282 IP zot.tiger.co.il.domain > 192.83.205.242.1027:  19255 NXDomain
 0/1/0 (121)
23:51:34.308319 IP 192.83.137.239.1041 > 192.83.205.242.telnet: . ack 2775 win 7
556
23:51:34.308444 IP 192.83.205.242.telnet > 192.83.137.239.1041: P 2775:3237(462)
 ack 0 win 5840
23:51:34.508392 IP 192.83.137.239.1041 > 192.83.205.242.telnet: . ack 3237 win 8
736
23:51:34.508518 IP 192.83.205.242.telnet > 192.83.137.239.1041: P 3237:3419(182)
 ack 0 win 5840
23:51:34.531317 IP 192.83.137.239.1041 > 192.83.205.242.telnet: P 0:1(1) ack 341
9 win 8554
23:51:34.531448 IP 192.83.205.242.telnet > 192.83.137.239.1041: P 3419:3601(182)
 ack 1 win 5840

39 packets captured
39 packets received by filter
0 packets dropped by kernel
OS900#
```

# TELNET

## Definition

TELNET is a TCP/IP protocol terminal emulation software program that is run on a host.

## Purpose

TELNET is used to connect a host/client (e.g., PC) to a server (e.g., OS900) on a network (e.g., Ethernet).

## Sessions

### Limit

For security reasons, the number of concurrent TELNET sessions is limited to 10.

### Timeout

#### *Setting*

The default timeout for sessions is 5 minutes.

To set a new timeout:

1. Enter **configure terminal** mode.
2. Enter **line** mode by invoking the command:
   **line vty**
3. Invoke the command:
   **exec-timeout global|current-session <0-35791>**
   where,
   **global**: For all sessions
   **current-session**: For the current session
   **<0-35791>**: Timeout value in minutes. If no value is entered for this parameter, timeout is disabled.
4. To exit **line** mode (and to enter **configure terminal** mode), invoke the command **exit**.

Example

```
OS910(config-line)# exec-timeout global 20
ATTENTION: LOGOUT timeout is set to 20 min.
OS910(config-line)#
```

#### *Disabling*

To disable timeout for a session:

1. Enter **configure terminal** mode.
2. Enter **line** mode by invoking the command:
   **line vty**
3. Invoke the command:
   **no exec-timeout global|current-session**
   where,
   **global**: For all sessions
   **current-session**: For the current session
4. To exit **line** mode (and to enter **configure terminal** mode), invoke the command **exit**.

Example

```
OS910(config-line)# no exec-timeout global
OS910(config-line)# ATTENTION: LOGOUT timeout is disabled.
OS910(config-line)#
```

***Default***

To set the timeout value for a session to the default (5 minutes):

1. Enter **configure terminal** mode.
2. Enter **line** mode by invoking the command:
   **line vty**
3. Invoke the command:
   **exec-timeout global|current-session default**
   **global**: For all sessions
   **current-session**: For the current session
4. To exit **line** mode (and to enter **configure terminal** mode), invoke the command **exit**.

Example

```
OS910(config-line)# exec-timeout global default
OS910(config-line)# ATTENTION: LOGOUT timeout is set to 5 min.
OS910(config-line)#
```

***Viewing***

To view the current setting of the timeout value for a session (in minutes):

1. Enter **configure terminal** mode.
2. Enter **line** mode by invoking the command:
   **line vty**
3. Invoking the command:
   **show line vty configuration**

Example

```
OS910(config-line)# show line vty configuration
LINE VTY CONFIGURATION:
Automatic logout is enabled, timeout value - 20.
Current session automatic logout timeout is equal to the global one.
OS910(config-line)#
```

## Connection

For TELNET to work, the appropriate installation must be performed as described in the section *TELNET/SSH Station or SNMP NMS*, page *81*.

To make a TELNET connection:

1. Enter **enable** mode.
2. Invoke the command:
   **telnet WORD PORT**
   where,
   **WORD**: IP address or DNS hostname of a remote OS900.
   **PORT**: TCP Port number.

In response, TELNET prompts you to enter a valid username and password before permitting access.

## Example

The example below shows how to invoke a TELNET connection.

```
OS900# telnet 192.23.76.158 44
OS900#
```

# Secure Shell (SSH)

## Version

### Custom Support

By default, the OS900 supports SSH version 1 and 2.

To set the OS900 to support only SSH version 2:

1. Enter **boot** mode (under **configure terminal** mode).
2. Invoke the command:
   **sshd-protocol-version 2**
3. To make the setup run-time, invoke the command:
   **write memory**
   Or
   **write file [NAME]**
   where,
   **[NAME]**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **system.conf**.

### Default Support

To revert to the default support for SSH versions (i.e., 1 and 2):

1. Enter **boot** mode (under **configure terminal** mode).
2. Invoke the command:
   **no sshd-protocol-version**
3. To make the setup run-time, invoke the command:
   **write memory**
   Or
   **write file [NAME]**
   where,
   **[NAME]**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **system.conf**.

## Connection

Secure Shell (SSH) is like TELNET but offers security beyond just username and password. SSH protects a network from IP spoofing, IP source routing, and DNS spoofing. An attacker that has managed to take over a network can at most force SSH to disconnect. The attacker cannot capture the traffic or hijack the connection when encryption is enabled.

The limit on the number of concurrent sessions and the timeout is the same as for TELNET. For details, refer to the section *Sessions*, page *776*.

To perform an SSH connection:

1. Enter **enable** mode.
2. Invoke the command:
   **ssh USER_HOSTNAME**
   where,
   **USER_HOSTNAME**: Username@Host (e.g., **admin@197.38.44.85**).

In response, SSH prompts you to enter a valid username and password before permitting access.

The example below shows how to invoke an SSH connection.

```
OS900# ssh admin@197.38.44.85
OS900#
```

# Secure FTP

## General

Secure FTP (sometimes referred to as SSH File Transfer Protocol or simply SFTP) is an IETF network protocol that provides secure file access, file transfer, and file management functionality over any reliable data stream.

Although it is an extension of the SSH protocol version 2.0 (SSH-2), it is intended to be usable with other protocols. For example, it can be used for secure file transfer over TLS or for transfer of management information in VPN applications.

This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

Unlike SCP transfer, SFTP transfer may be aborted without causing the session to be terminated.

## Enabling

To enable the OS900 to function as an SFTP server:

1. Enter **boot** mode (under **configure terminal** mode).
2. Invoke the command:
   **sftp-server**
3. To make the setup run-time, invoke the command:
   **write memory**
   Or
   **write file [NAME]**
   where,
   **[NAME]**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **system.conf**.

## Disabling

This is the default mode.

To disable the OS900 from functioning as an SFTP server:

1. Enter **boot** mode (under **configure terminal** mode).
2. Invoke the command:
   **no sftp-server**
3. To make the setup run-time, invoke the command:
   **write memory**
   Or
   **write file [NAME]**
   where,
   **[NAME]**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **system.conf**.

# View Mode Commands

## General

Following successful login, the system prompt (e.g., `OS910>`) will appear to indicate entry into view mode. By default, the commands accessible in this mode enable the user to perform actions external to the OS900.

## Enabling

To enable display also of commands that provide information internal to the OS900:

1. Enter **`boot`** mode (under **`configure terminal`** mode).
2. Invoke the command:
   **`view-commands enable`**
3. To make the setup run-time, invoke the command:
   **`write memory`**
   Or
   **`write file [NAME]`**
   where,
   **`[NAME]`**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **`system.conf`**.

## Disabling

This is the default mode.

To disable display of commands that provide information internal to the OS900.

1. Enter **`boot`** mode (under **`configure terminal`** mode).
2. Invoke the command:
   **`no view-commands enable`**
3. To make the setup run-time, invoke the command:
   **`write memory`**
   Or
   **`write file [NAME]`**
   where,
   **`[NAME]`**: Name of the file in which the configuration of the OS900 is to be saved. By default (i.e., if this optional argument is not specified), the configuration is saved in the file **`system.conf`**.

# Address Resolution Protocol (ARP)

## General

Address Resolution Protocol (ARP) is a protocol for mapping an IP address (32-bit) to the MAC address (48-bit) of a host machine.

An ARP table maintains current maps of MAC addresses to IP addresses.

## Principle of Operation

When an incoming packet destined for a host machine arrives at the OS900, the OS900 uses the ARP program to search for the MAC address that matches the IP address. If it finds the MAC address, it provides it adjusts the packet to the right length and format and sends it to the machine. If it does not find the IP address, ARP broadcasts a request packet in a special format to all the host machines on the LAN to try to find a host machine with the specific IP address. If a host machine recognizes the IP address as its own, it responds positively. The OS900 then updates its ARP table accordingly and sends the packet to the host with this MAC address.

Reverse ARP (RARP) is used by host machines to obtain their IP address from a gateway's ARP cache.

## Adding/Modifying an ARP Table Entry

An entry may be made into the ARP Table by the user as follows:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`arp HOSTNAME A:B:C:D:E:F perm|temp [INTERFACE]`**
   where,
   **`HOSTNAME`**: Hostname or IP address for the new ARP entry

**A:B:C:D:E:F**: MAC address in new ARP entry.

**perm**: Permanent entry, i.e., stays in the ARP table so long as the OS900 keeps running.

**temp**: Temporary entry, i.e., subject to aging – see section *Aging*, page *112*.

**INTERFACE**: (optional) VLAN Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095

The example below shows how to make an ARP entry.

```
OS900(config)# arp 192.200.137.108 00:11:22:33:44:55 perm vif65
OS900#
```

## Deleting ARP Table Entries

To delete entries in the ARP Table:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no arp all|HOSTNAME [INTERFACE]**

   where,

   **all**: All existing entries in the ARP Table.

   **HOSTNAME**: Hostname or IP address in the existing entry of the ARP Table

   **INTERFACE**: VLAN Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095

The example below shows how to delete an ARP entry.

```
OS900(config)# no arp 192.200.137.108 vif65
OS900#
```

## Viewing the ARP Table

To view the ARP Table:

1. Enter **enable** mode.
2. Invoke the command:

   **show arp [RESOLVE] HOSTNAME INTERFACE**

   where,

   **RESOLVE**: (optional) **res** or **nres**.

   **res** – Resolve hostname in the existing ARP Table entries.

   **nres** – Do not resolve hostname in the existing ARP Table entries

   **HOSTNAME**: Hostname or IP address in the existing ARP Table entries

   **INTERFACE**: VLAN Interface ID having the format **vifX**, where **X** is a decimal number in the range 1-4095

The examples below shows how to display the ARP Table .

Example 1

```
OS900# show arp
? (192.168.130.132) at 00:0E:0C:4B:AE:41 [ether] on vif5
? (193.88.136.20) at 00:04:90:00:17:19 [ether] on vif5
? (193.88.136.6) at 00:01:02:12:7C:61 [ether] on vif5
? (193.88.136.18) at 00:11:11:F1:EA:C4 [ether] on vif5
? (10.91.136.9) at 00:20:1A:00:D5:91 [ether] on vif5
```

Example 2

```
OS900# show arp res 192.88.136.102
Apollo.Hi-tech.com (10.90.136.15) at 00:01:02:AE:C5:A1 [ether] on vif38
OS900#
```

# Configuration File Management

## Configuration File Location

The startup system configuration file is stored at:

**`/usr/local/etc/System.conf`**

## Editing & Saving Configuration File

To edit the System Configuration File directly:

1. Enter **`enable`** mode.
2. Type **`linux`** to enter the Linux Operating System.
3. In response to the Linux prompt **`$`**, type **`vi/usr/local/etc/System.conf`** to open the file (for editing).

To save System Configuration File after editing in the startup system configuration file (in permanent/flash memory):

1. Type **`su`**.
2. Enter the root password.
3. Type /usr/local/nbase/bin/flush-conf.sh
4. Type reboot. To run the system with the changed configuration.

The user inputs (in bold) and the system responses in carrying out the procedure using the CLI are as follows:

```
OS900> enable
OS900# linux
$ vi/usr/local/etc/System.conf
$
$ su
Password:
# /usr/local/nbase/bin/flush-conf.sh
# reboot
```

# Memory Management

## Viewing Memory

The Linux OS memory usage is oriented to enhance performance and enable maximum use of free memory in the OS900. By design, the Linux OS will use ALMOST ALL available memory for internal use of buffers and cache, as can be seen for ‘buffer’ and ‘cache’ in the display obtained by invoking the command **`show memory`**. This behavior enables the Linux OS to cache and buffer disk I/O and keep most data resident in memory as long as possible. The purpose is to minimize fetching of files and data from the disk.

As a result, regardless of the amount of OS900 resident RAM Memory, the usage pattern will be the same. Free memory is regarded by the Linux OS as “a complete waste”, so for performance reasons the "buffers" and "cached" figures should be as high as possible. It enables Linux OS to make the best usage of memory and enhances system performance.

In case an OS900 process needs to use memory for whatever reason, the memory space that is used for disk cache and buffers is freed immediately.

The following is a **`show memory`** dump collected on an OS900.

```
OS900(config)# show memory
        total:    used:    free:  shared: buffers:  cached:
Mem:  30183424 28778496  1404928        0  4423680 14901248
Swap:        0        0        0
MemTotal:        29476 kB
MemFree:          1372 kB
MemShared:           0 kB
Buffers:          4320 kB
Cached:          14552 kB
```

```
SwapCached:           0 kB
Active:            5708 kB
Inactive:         18892 kB
HighTotal:            0 kB
HighFree:             0 kB
LowTotal:         29476 kB
LowFree:           1372 kB
SwapTotal:            0 kB
SwapFree:             0 kB
Committed_AS:     21848 kB
OS900(config)#
```

By taking those figures and recalculating as shown in *Table 35*, below, it is easy to see that the "real free" memory value stabilized around 63% of the Total memory.

**Table 35: Memory Space Usage**

| Total | Cached | Buffers | Free | Used | Buffer + Cache | Real Used | Real Free | % Real Free |
|---|---|---|---|---|---|---|---|---|
| 260636672 | 86450176 | 70217728 | 12722176 | 247914496 | 156667904 | 91246592 | 169390080 | 64.991% |
| 260636672 | 75616256 | 90058752 | 5738496 | 254898176 | 165675008 | 89223168 | 171413504 | 65.767% |
| 260636672 | 86441984 | 68837376 | 4513792 | 256122880 | 155279360 | 100843520 | 159793152 | 61.309% |
| 260636672 | 85377024 | 70889472 | 4694016 | 255942656 | 156266496 | 99676160 | 160960512 | 61.757% |
| 260636672 | 88330240 | 69058560 | 16805888 | 243830784 | 157388800 | 86441984 | 174194688 | 66.834% |

where:
**Real Free** = Free + buf + cache
**Real Used** = Total – real free
**% Real Free** = Real free / Total x 100

To view the different memory banks (and current occupancy in kB):

1. Enter **`enable`** mode.
2. Invoke the command **`show memory`**.

Below is an example display of the OS900 outputs on a CLI screen in response to the command **`show memory`**.

```
OS900# show memory
        total:    used:    free:  shared: buffers:  cached:
Mem:  130863104 85483520 45379584        0        0 27783168
Swap:        0        0        0
MemTotal:       127796 kB
MemFree:         44316 kB
MemShared:           0 kB
Buffers:             0 kB
Cached:          27132 kB
SwapCached:          0 kB
Active:          10672 kB
Inactive:        16584 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       127796 kB
LowFree:         44316 kB
SwapTotal:           0 kB
SwapFree:            0 kB
OS900#
```

## Viewing Processes

### Processes

To view memory processes, invoke the command **show processes**. The values in the RSS column indicate the total amount of physical memory used by each process.

The following is a **show processes [FLAGS]** capture collected on an OS900.

To view the current processes in the OS900:

1. Enter **enable** mode.
2. Invoke the command show processes [FLAGS].

Example

```
OS910# show processes
  PID  Uid     VmSize Stat Command
    1 root        624 S   init
    2 root            SWN [ksoftirqd/0]
    3 root            SW< [events/0]
    4 root            SW< [khelper]
    5 root            SW< [kthread]
    6 root            SW< [kblockd/0]
    7 root            SW  [pdflush]
    8 root            SW  [pdflush]
   10 root            SW< [aio/0]
    9 root            SW  [kswapd0]
   11 root            SW  [0000:00:18.0]
   12 root            SW  [mtdblockd]
  124 root            SWN [jffs2_gcd_mtd0]
  133 root        472 S   /sbin/klogd
  136 daemon      352 S   /sbin/portmap
  139 root        468 S   /usr/sbin/cron
  355 root       2004 S   initd -t 10 -i /usr/local/etc/System.conf -dh
  356 root       1260 S   uid_task
  357 root       1260 S   uid_task
  358 root       1260 S   uid_task
  359 root       1260 S   uid_task
  360 root       1260 S   uid_task
  361 root       1260 S   uid_task
  362 root      19268 S   pssExe
  363 root      19268 S   pssExe
  364 root      19268 S < pssExe
  365 root      19268 S   pssExe
  366 root      19268 S < pssExe
  367 root      19268 S   pssExe
  368 root      19268 S   pssExe
  369 root      19268 S   pssExe
  370 root      19268 S < pssExe
  371 root      19268 S < pssExe
  372 root      19268 S   pssExe
  373 root      19268 S   pssExe
```

```
  374 root       2632 S   ssys
  393 root        496 S   /sbin/syslogd -m 0
  397 root       1808 S   sport_srv
  398 root       1268 S   sfib
  399 root       1496 S   smfib
  400 root       1180 S   vctd
  401 root       1268 S   sfib
  402 root       1268 S   sfib
  403 root       2472 S   spf
  404 root       1300 S   svrrp
  405 root       1380 S   snetlink
  406 root       1380 S   snetlink
  407 root       1380 S   snetlink
  408 root       1352 S   slei
  409 root       1360 S   rtrd
  410 root       2724 S   sif
  411 root       2032 S   mstpd -d
  412 root       1220 S   lacpd
  413 root       1668 S   udldd
  414 root       1400 S   ethoamd
  415 root       1120 S   sdhcp
  416 root       1120 S   sdhcp
  417 root       1120 S   sdhcp
  418 root       1364 S   snetutil
  419 root       1388 S   smrd
  420 root       1388 S   smrd
  421 root       1388 S   smrd
  422 root       2268 S   sflow_mgr
  423 root       1056 S   mplsoam
  424 root       4196 S   snmpd -f -L -s udp:161
  425 root        896 S   saaa
  426 root       1072 S   sntp
  427 root       3468 S   osmd
  428 root       3468 S   osmd
  429 root       3468 S   osmd
  430 root       2108 S   zebos
  431 root       2284 S   ripd
  432 root       2852 S   bgpd
  433 root       2320 S   isisd
  434 root       2584 S   ospfd
  443 root       1116 S   /usr/sbin/sshd
  448 root        848 S   /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -reuse
  450 admin      1096 S   /bin/sh /usr/local/nbase/bin/adminsh
  452 admin      5476 S   /usr/local/nbase/bin/vtysh
  457 admin      5476 S   /usr/local/nbase/bin/vtysh
  458 admin      5476 S   /usr/local/nbase/bin/vtysh
```

```
  473 admin       532 S   more
  474 admin       824 R   ps aux
OS910#
```

**Top Processes and Memory**

To view *continually updated* (automatically refreshed) memory and CPU usage by processes running in the OS900:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show top-processes`**

Example

```
OS900# show top-processes
top - 11:48:44 up 6 min,  1 user,  load average: 0.03, 0.10, 0.06
Tasks:  82 total,   2 running,  80 sleeping,   0 stopped,   0 zombie
Cpu(s):  3.5% us,  3.9% sy,  0.0% ni, 92.6% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:    257416k total,    94452k used,   162964k free,    10324k buffers
Swap:        0k total,        0k used,        0k free,    27764k cached

  PID USER       PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
  471 admin      15   0  2560 1068  832 R  5.5  0.4   0:00.09 top
    1 root       16   0  2656  624  532 S  0.0  0.2   0:03.03 init
    2 root       39  19     0    0    0 S  0.0  0.0   0:00.00 ksoftirqd/0
    3 root       10  -5     0    0    0 S  0.0  0.0   0:00.00 events/0
    4 root       10  -5     0    0    0 S  0.0  0.0   0:00.01 khelper
    5 root       18  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
    6 root       10  -5     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
    7 root       20   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
    8 root       15   0     0    0    0 S  0.0  0.0   0:00.00 pdflush
   10 root       10  -5     0    0    0 S  0.0  0.0   0:00.00 aio/0
    9 root       25   0     0    0    0 S  0.0  0.0   0:00.00 kswapd0
   11 root       25   0     0    0    0 S  0.0  0.0   0:00.00 0000:00:18.0
   12 root       15   0     0    0    0 S  0.0  0.0   0:01.35 mtdblockd
  124 root       30  10     0    0    0 S  0.0  0.0   0:00.00 jffs2_gcd_mtd0
  133 root       16   0  2656  472  376 S  0.0  0.2   0:00.17 klogd
  136 daemon     21   0  1652  352  276 S  0.0  0.1   0:00.01 portmap
  139 root       16   0  1696  468  344 S  0.0  0.2   0:00.00 cron
OS900#
```

To exit the display, invoke the command **`exit`** or **`quit`**.

# Multicast Destination MAC Addresses

To display the registered multicast MAC addresses of packets that will be forwarded to all hosts on the network:

1. Enter **`enable`** mode.
2. Invoke the command **`show multicasts`**.

Example

```
OS900# show multicasts
indx interface_name  dmi_u dmi_g dmi_address
2    eth0            1     0     01005e000001
5    vif90           1     0     01005e000001
OS900#
```

The example above shows such a destination MAC address (under the heading `dmi_address`) common to the out-of-band interface `eth0` and the inband interface `vif90`.

# Debug Information

## Purpose

The debug information utility is used to obtain debug information on System Events.

## System Events

Examples of system events are: Link up, Link down, Interface up, Interface down.

### Activating Display

To activate the display of system events on the CLI screen each time a system event occurs:

1. Enter **`enable`** mode.
2. Invoke the command **`debug event`**.

### Deactivating Display

To deactivate the display of system events on the CLI screen:

1. Enter **`enable`** mode.
2. Invoke the command **`no debug event`**.

# Linux Tasks

To view the Linux tasks being performed in real time:

1. Enter **`enable`** mode.
2. Invoke the command:
   **`show top-processes`**

To exit monitoring (and freeze the display), press Ctrl C.

# Fan Control

## General

Fan control applies to all OS900 models except OS906, OS912 and OS930, in which the fan/s is/are set to run constantly.

The user can cause the cooling fan/s in an OS900 to be turned on and off at specific ambient temperatures. In an environment having a suitable temperature, this capability can be used to run the OS900 silently as well as to save on power.

## Setting Fan-on and Fan-off Temperatures

To set the fan-on and fan-off temperatures:

1. Enter **`configure terminal`** mode.
2. To set the fan-on and fan-off temperatures in degrees

   Celsius (Centigrade)

   Invoke the command:

   **`fan temperature <1-65> <1-65>`**

   where,

   **`<1-65>`**: (First appearance) Temperature (in $^{o}$C) at which the fan/s is/are to be turned ***on***.

   Default: For OS904/***A***C, OS904/***D***C: 60 $^{o}$C
   For OS910/***A***C, OS910-M/***A***C: 60 $^{o}$C
   For OS910/***D***C, OS910-M/***D***C: 45 $^{o}$C

   **`<1-65>`**: (Second appearance) Temperature (in $^{o}$C) at which the fan/s is/are to be turned ***off***.

   Default: For OS904/***A***C, OS904/***D***C: 50 $^{o}$C

For OS910/***A***C, OS910-M/***A***C: 57 °C
For OS910/***D***C, OS910-M/***D***C: 42 °C

Example

```
OS900(config)# fan temperature 53 49
OS900(config)#
```

Fahrenheit

Invoke the command:

**`fan temperature fahrenheit <34-149> <34-149>`**

where,

**`<34-149>`**: (First appearance) Temperature (in °F) at which the fan/s is/are to be turned ***on***.

Default: For OS904/***A***C, OS904/***D***C: 140 °F
For OS910/***A***C, OS910-M/***A***C: 140 °F
For OS910/***D***C, OS910-M/***D***C: 113 °F

**`<34-149>`**: (Second appearance) Temperature (in °F) at which the fan/s is/are to be turned ***off***.

Default: For OS904/***A***C, OS904/***D***C: 122 °F
For OS910/***A***C, OS910-M/***A***C: 134.6 °F
For OS910/***D***C, OS910-M/***D***C: 107.6 °F

Example

```
OS900(config)# fan temperature fahrenheit 100 85
OS900(config)#
```

### Viewing Fan-on and Fan-off Temperatures

To view the ambient temperatures at which the cooling fan/s is/are to be turned on and off:

1. Enter **`enable`** mode.
2. Invoke the following command:
   **`show fan`**

Example

```
OS900(config)# exit
OS900# show fan

Fan Configuration:
------------------
Fan On Temperature:  60C / 140F
Fan Off Temperature: 50C / 122F
OS900#
```

### Default Fan-on and Fan-off Temperatures

To set the fan-on and fan-off temperatures to the *default* values:

1. Enter **`configure terminal`** mode.
2. Invoke the command:
   **`no fan temperature`**

Example

```
OS900(config)# no fan temperature
OS900(config)#
```

# Technical Support Information

### Viewing

To view OS900 technical support information:

1. Enter **enable** mode.
2. Invoke the command:
   **show tech-support**

## Copying to a Server

To copy OS900 technical support information to an FTP or SCP server:

1. Enter **enable** mode.
2. Invoke the command:
   **copy tech-support (ftp|scp) SERVER REMOTE-DIR [USERNAME] [PASSWORD]**
   where,
   **ftp**: Use FTP protocol for copying.
   **scp**: Use SCP protocol for copying.
   **SERVER**: DNS Host name or IP address of the server.
   **REMOTE-DIR**: Full pathname to the directory on the server.
   **[USERNAME]**: Username for login.
   **[PASSWORD]**: Password for login.

# Exporting Data

## General

This utility is used to set the OS900 to periodically send a file containing data collected by the OS900 to a host.

Several independent exports can be configured by assigning different export names (IDs).

## Configuration

1. Enter **configure terminal** mode.
2. Name the export to be configured by invoking the command:
   **export NAME**
   where,
   **NAME**: Name for export to be configured.
   (To delete the export name invoke the command **no export NAME**.)
3. Specify the name to be given to the export file (file containing data collected by the OS900 and to be exported) by invoking either of the following commands:
   **client id ID**
   where,
   **ID**: ID of client. If the command **remote filename FILENAME** (described in the section *Filename*, page *790*) is not invoked, this ID is used as the *first* part of the name for the export file. The *second* part designates the data sample type (e.g., SC – service counter data, LB – loopback test results, DM – delay measurement, IP – IP SLA test results). The *third* part designates the date on which the file was exported in the format: **YYYYMMDDhhmmss**).
   (To delete the client ID invoke the command **no client id**.)
4. Specify the IP address or DNS hostname of the host that is to receive the export file by invoking the command:
   **server address (A.B.C.D|HOSTNAME)**
   where,
   **A.B.C.D**: IP address of the host.
   **HOSTNAME**: DNS name of the host.
   (To delete the IP address/DNS hostname invoke the command **no server address**.)

5. Specify the name of the directory on the host in which the file containing the export data is to be stored by invoking the command:
   **`remote dirname DIRNAME`**
   where,
   **`REMOTE-DIR`**: Full path to the directory on the host.
   (To delete the directory name invoke the command **`no remote dirname`**.)

## Optional Configuration Parameters

### Description

To enter an alphanumeric string that is to serve as a description of the export invoke the command:

**`description ...`**

where,

`...`: Alphanumeric string. (The string can be a single word or several words separated by blank spaces or interconnected with hyphens and/or underscores.)

(To delete the description invoke the command **`no description`**.)

### Filename

To specify a name for the file to which the export data is to be copied invoke the command:

**`remote filename FILENAME`**

where,

**`FILENAME`**: Name for the file to which the export data is to be copied.

(To delete the filename, invoke the command **`no remote filename`**.)

### Username

To specify a username required at the host in order to access the export file invoke the command:

**`remote username USERNAME`**

where,

**`USERNAME`**: Login username at host. (Default: **`anonymous`**)

(To delete the filename, invoke the command **`no remote username`**.)

### Password

To define a password required at the host in order to access the export file invoke the command:

**`remote password PASSWORD`**

where,

**`PASSWORD`**: Login password at host.

(To delete the password, invoke the command **`no remote password`**.)

### Protocol

To select the protocol to be used in transferring the export file invoke the command:

**`transfer protocol (ftp|scp)`**

where,

**`ftp`**: File Transfer Protocol (default).

**`scp`**: Secure Copy protocol.

(To revert to the default protocol, **`ftp`**, invoke the command **`no transfer protocol`**.)

### Size

To set the number of data samples (to be entered in the export file) before they are sent (to the host) invoke the command:

**`transfer block-size <1-2000>`**

where,

**<1-2000>**: Number of data samples to be sent to the export file (Default: **10**).

(To reset the number of data samples to the default (**10**), invoke the command **no transfer block-size**.)

| **Note** |
|---|
| Sets of data samples are sent periodically to the export file in which they are accumulated. |

### Time Interval

To set the time interval between the sets of data samples (default: **once**) invoke the command:

```
sample interval
(once|month|week|day|12hrs|8hrs|6hrs|4hrs|2hrs|1hr|30mins|15mins|10
    mins|5mins|2mins|1min)
```

(To reset the time interval to the default (**once**), invoke the command **no sample interval**.)

### Start

To set the start date & time for sending sets of data samples invoke the command:

```
start time DATE-AND-TIME
```

where,

**DATE-AND-TIME**: Start date & time for sending sets of data samples to the export file. Format: **MM/DD/YYYY-hh:mm:ss**. (Default: start immediately)

(To reset the start date & time to the default (start immediately), invoke the command **no start time**.)

### Enabling

To enable export invoke the command:

```
enable
```

## Stopping Exports

To stop export:

1. Enter **configure terminal** mode.
2. Enter the mode of the export (by invoking the command **export NAME**.)
3. Invoke the command:
   ```
   no enable
   ```

## Deleting Exports

### Specific

To delete a specific export:

1. Enter **configure terminal** mode.
2. Invoke the command:
   ```
   no export NAME
   ```
   where,

   **NAME**: ID for export to be configured.

### All

To delete all existing exports:

1. Enter **configure terminal** mode.
2. Invoke the command:
   ```
   no export
   ```

# Sleep

To pause operation of the OS900 for a user-specified period of time:

1. Enter **`enable`** mode.
2. Invoke the command:

   **`sleep <1-3600>`**

   where,

   **`<1-3600>`**: Sleep period (in seconds) to be selected from the range 1 to 3600.

# Debugging

## Information

### Purpose

The debug information utility is used to obtain debug information on the following:

- System Events
- BGP Events
- ERPS Events
- Ethernet OAM Events
- Interface Events
- ISIS Events
- LACP Events
- NSM Routing Events
- OSPF Events
- Port Events
- RIP Events
- SNMP Events
- Spanning-Tree Events

The information is logged in the Syslog file at: **/var/log/messages**.

### System Events

***Activating Display***

To activate display of system events on the CLI screen:

1. Enter **`enable`** mode.
2. Invoke the command **`debug event`**.

***Deactivating Display***

To deactivate display of system events on the CLI screen:

1. Enter **`enable`** mode.
2. Invoke the command **`no debug event`**.

### BGP Events

***Activating Display***

To activate display of BGP events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   ```
   debug bgp [events|filters|fsm|keepalives|nsm|(target
   [all|cli|console|current-session|log])|(updates
   [in|out])]
   ```

   where,

**events**: BGP events
**filters**: BGP filters
**fsm**: BGP finite state machine
**keepalives**: BGP keepalives
**nsm**: Network Service Module (NSM) message
**target**: Target of traces
  **all**: All targets
  **cli**: CLI (TELNET/SSH) sessions
  **console**: System console
  **current-session**: Current CLI session
  **log**: System log
**updates [in|out]**: BGP updates inbound|outbound
  **in**: Inbound updates
  **out**: Outbound updates

***Deactivating Display***

To deactivate display of BGP events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no debug bgp [events|filters|fsm|keepalives|nsm|target|updates]**

### ERPS Events

***Activating Display***

To activate display of ERPS events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **debug erp <0-7> (fsm|events|raps-tx|raps-rx|ports|timers|ccm|general)**
   where,
   **fsm**: ERPS finite state machine
   **events**: ERPS events
   **raps-tx**: Transmitted R-APS
   **raps-rx**: Received R-APS
   **ports**: Ring West and East ports
   **timers**: ERP timers (Guard timer,Hold-off timer)
   **ccm**: CCM activation
   **general**: General events related to ERPS

***Deactivating Display***

To deactivate display of ERPS events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no debug erp <0-7> (fsm|events|raps-tx|raps-rx|ports|timers|ccm|general)**

### Ethernet OAM Events

***Activating Display***

To activate display of IEEE 802.1ag/ITU-T Y.1731 OAM events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:

**debug ethernet oam domain <0-7> service NUMBER interfaces|(mep <1-4095> port <1-223> activation|ccm-freeze|dmm|fng|rx-ccm|tx-ccm)**

where,

**<0-7>**: Domain level (Integer)

**NUMBER**: Index of MA as a decimal or hexadecimal number from 1 to 65535

**<1-4095>**: Local MEP ID to be selected from the range 1 to 4095

**<1-223>**: Software port number

**activation**: Port activation

**ccm-freeze**: CCM Freezing

**dmm**: Delay Measurement/LoopBack tests start/stop

**fng**: Fault Notification Generator

**rx-ccm**: CCM PDU Reception

**tx-ccm**: CCM PDU Transmission

Or

**debug ethernet oam target all|cli|console|current-session|log**

where,

**all**: All targets

**cli**: CLI (TELNET/SSH) sessions

**console**: System console

**current-session**: Current CLI session

**log**: System log

***Deactivating Display***

To deactivate display of IEEE 802.1ag/ITU-T Y.1731 OAM events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no debug ethernet oam domain <0-7> service NUMBER interfaces|(mep <1-4095> port <1-223> activation|ccm-freeze|dmm|fng|rx-ccm|tx-ccm)**

**Interface Events**

***Activating Display***

To activate display of Interface events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **debug interface target (all|cli|console|current-session|log)**

   where,

   **all**: All targets

   **cli**: CLI (TELNET/SSH) sessions

   **console**: System console

   **current-session**: Current CLI session

   **log**: System log

***Deactivating Display***

To deactivate display of Interface events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:

   **no debug interface target (all|cli|console|current-session|log)**

### IS-IS Events

#### *Activating Display*

To activate display of IS-IS events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **debug isis (events|ifsm|lsp|nfsm|nsm|pdu [in|out]|target (all|cli|console|current-session|log)**
   where,
   **events**: IS-IS Events
   **ifsm**: IS-IS Interface Finite State Machine
   **lsp**: IS-IS Link State PDU
   **nfsm**: IS-IS Neighbor Finite State Machine
   **nsm**: IS-IS Network Service Module (NSM) information
   **pdu**: IS-IS Protocol Data Unit
   **in**: Inbound ISIS PDUs
   **out**: Outbound ISIS PDUs
   **spf**: IS-IS SPF Calculation
   **target**: Target of traces
   **all**: All targets
   **cli**: CLI (TELNET/SSH) sessions
   **console**: System console
   **current-session**: Current CLI session
   **log**: System log

#### *Deactivating Display*

To deactivate display of IS-IS events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **no debug isis (events|ifsm|lsp|nfsm|nsm|pdu [in|out]|target (all|cli|console|current-session|log)**

### LACP Events

#### *Activating Display*

To activate display of LACP events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
   **debug lacp port (link|mux|rx|sync|tx)|target (all|cli|console|current-session|log)**
   where,
   **port**: Physical port
   **link**: Link change events
   **mux**: MUX state change events
   **rx**: Received PDUs
   **sync**: Synchronization
   **tx**: Transmitted PDUs
   **target**: Target of traces
   **all**: All targets
   **cli**: CLI (TELNET/SSH) sessions
   **console**: System console
   **current-session**: Current CLI session

**log**: System log

***Deactivating Display***

To deactivate display of LACP events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
**no debug lacp port (link|mux|rx|sync|tx)|target (all|cli|console|current-session|log)**

**NSM Routing Events**

***Activating Display***

To activate display of Network Service Module (NSM) routing events debug information on the CLI screen:

1. Enter **configure terminal** mode.
2. Enable logging of Operative Software events as described in the section *Logging of Events*, page *116*.
3. Invoke the command:
**debug nsm events|kernel|(packet [recv|send [detail]])|(target (all|cli|console|current-session|log))**
where,
**events**: NSM events
**kernel**: NSM between kernel and interface
**packet**: NSM packets
**recv**: Received packets
**detail**: Details
**send**: Sent packets
**detail**: Details
**target**: Target of traces
**all**: All targets
**cli**: CLI (TELNET/SSH) sessions
**console**: System console
**current-session**: Current CLI session
**log**: System log

***Deactivating Display***

To deactivate display of NSM events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
**no debug nsm events|kernel|packet|(target (all|cli|console|current-session|log))**

**OSPF Events**

***Activating Display***

To activate display of OSPF events on the CLI screen:

1. Enter **configure terminal** mode.
2. Invoke the command:
**debug ospf**
**(event [abr|asbr|lsa|nssa|os|router|vl])|**
**(ifsm [events|status|timers])|**
**(lsa [flooding|generate|install|maxage|refresh])|**
**(nfsm [events|status|timers])|**
**(nsm [interface|redistribute])|**
**(packet [all [[send|recv] [detail]]]|dd [[send|recv] [detail]]]|hello [[send|recv] [detail]]]|ls-ack [[send|recv]**

**[detail]]]|ls-request [[send|recv] [detail]]]|ls-update]**
**[[send|recv] [detail]]])|**
**(prioritized-treatment [inactivity-timer|retransmit-interval|lsa-pacing|throttling-adjacencies])|**
**(route [ase|ia|install|spf])|**
**(target [all|cli|console|current-session|log])**

where,

- **event**: OSPF Events
  - **abr**: OSPF Area Border Router events
  - **asbr**: OSPF Autonomous System Boundary Router events
  - **lsa**: OSPF Link State Advertisement events
  - **nssa**: OSPF Not-So-Stubby Area events
  - **os**: OSPF OS interaction events
  - **router**: Other router events
  - **vl**: OSPF Virtual Link events
- **ifsm**: OSPF Interface State Machine events
  - **events**: IFSM Event Information
  - **status**: IFSM Status Information
  - **timers**: IFSM Timer Information
- **lsa**: OSPF Link State Advertisement events
  - **flooding**: LSA Flooding
  - **generate**: LSA Generation
  - **install**: LSA Installation
  - **maxage**: LSA MaxAge processing
  - **refresh**: LSA Refreshment
- **nfsm**: OSPF Neighbor Finite State Machine (NFSM) events
  - **events**: NFSM Events
  - **status**: NFSM Status
  - **timers**: NFSM Timer
- **nsm**: OSPF Network Service Module (NSM) events
  - **interface**: NSM interface
  - **redistribute**: NSM redistribute
- **packet**: OSPF Link State Advertisement events
  - **all**: All OSPF packets
    - **send**: Packets sent
      - **detail**: Details
    - **recv**: Packets received
      - **detail**: Details
  - **dd**: OSPF Database Description
  - **hello**: OSPF Hello
  - **ls-ack**: OSPF Link State Acknowledgment
  - **ls-request**: OSPF Link State Request
  - **ls-update**: OSPF Link State Update
- **prioritized-treatment**: Prioritized-treatment (per RFC4222)
  - **inactivity-timer**: Prioritized-treatment Inactivity Timer (RFC improvement recommendation 2)
  - **retransmit-interval**: Prioritized-treatment Retransmit-Interval (RFC improvement recommendation 3)
  - **lsa-pacing**: Prioritized-treatment Link-State-Advertisement Pacing (RFC improvement recommendation 4)

**`throttling-adjacencies`**: Prioritized-treatment Throttling-Adjacencies (RFC improvement recommendation 5)

**`route`**: OSPF route

**`ase`**: External route (calculated)

**`ia`**: Inter-Area route (calculated)

**`install`**: Route installation

**`spf`**: Shortest Path First (SPF) (calculated)

**`target`**: Target of traces

**`all`**: All targets

**`cli`**: CLI (TELNET/SSH) sessions

**`console`**: System console

**`current-session`**: Current CLI session

**`log`**: System log

***Deactivating Display***

To deactivate display of OSPF events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

```
no debug ospf
(event [abr|asbr|lsa|nssa|os|router|vl])|
(ifsm [events|status|timers])|
(lsa [flooding|generate|install|maxage|refresh])|
(nfsm [events|status|timers])|
(nsm [interface|redistribute])|
(packet [all [[send|recv] [detail]]]|dd [[send|recv]
[detail]]]|hello [[send|recv] [detail]]]|ls-ack [[send|recv]
[detail]]]|ls-request [[send|recv] [detail]]]|ls-update]
[[send|recv] [detail]]])|
(prioritized-treatment [inactivity-timer|retransmit-
interval|lsa-pacing|throttling-adjacencies])|
(route [ase|ia|install|spf])|
(target [all|cli|console|current-session|log])
```

**Port Events**

***Activating Display***

To activate display of Port events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

```
debug port target (all|cli|console|current-session|log)
```

where,

**`target`**: Target of traces

**`all`**: All targets

**`cli`**: CLI (TELNET/SSH) sessions

**`console`**: System console

**`current-session`**: Current CLI session

**`log`**: System log

***Deactivating Display***

To deactivate display of Port events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

```
no debug port target (all|cli|console|current-
session|log)
```

### RIP Events

#### *Activating Display*

To activate display of RIP events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`debug rip events|nsm|packet [recv|send]|target (all|cli|console|current-session|log)`**

   where,

   **`events`**: RIP Events

   **`nsm`**: RIP NSM information

   **`packet`**: RIP packets information

   **`recv`**: Received packets

   **`detail`**: Details

   **`send`**: Sent packets

   **`detail`**: Details

   **`target`**: Target of traces

   **`all`**: All targets

   **`cli`**: CLI (TELNET/SSH) sessions

   **`console`**: System console

   **`current-session`**: Current CLI session

   **`log`**: System log

#### *Deactivating Display*

To deactivate display of RIP events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`no debug rip events|nsm|packet [recv|send]|target (all|cli|console|current-session|log)`**

### SNMP Events

#### *Activating Display*

To activate display of SNMP events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`debug snmp target (all|cli|console|current-session|log)|trace (all|authentication|gen-traps|provision|rmon|spec-traps)`**

   where,

   **`target`**: Target of traces

   **`all`**: All targets

   **`cli`**: CLI (TELNET/SSH) sessions

   **`console`**: System console

   **`current-session`**: Current CLI session

   **`log`**: System log

   **`trace`**: Trace entities

   **`all`**: All traps & Authentication failed cases

   **`authentication`**: Authentication failed cases

   **`gen-traps`**: All generic traps to be sent

   **`provision`**: Provision

   **`rmon`**: RMON entities lifetime

   **`spec-traps`**: All specific traps to be sent

***Deactivating Display***

To deactivate display of SNMP events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`no debug snmp target (all|cli|console|current-session|log)|trace (all|authentication|gen-traps|provision|rmon|spec-traps)`**

**Spanning-Tree Events**

***Activating Display***

To activate display of Spanning-Tree events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

   **`debug spanning-tree (instance <0-63> prs|root-change|port (PORTS-GROUP c|f|h|pim|prt|pst|tcm))|(port (PORTS-GROUP bdm|ppm|prx|ptx|rx|sniffer|tx))|(target (all|cli|console|current-session|log))`**

   where,

   **`instance`**: Instance debug

   **`<0-63>`**: ID of the MSTP instance

   **`prs`**: Port Role Selection state machine

   **`root-change`**: Root change events (default)

   **`port`**: Ports debug

   **`PORTS-GROUP`**: Group of Ports

   **`c`**: Topology Change bit transmission

   **`f`**: Learning table flush events

   **`h`**: Hardware port MSTP state changes

   **`pim`**: Port Information state machine

   **`prt`**: Port Role Transition state machine

   **`pst`**: Port State Selection state machine

   **`tcm`**: Port Topology Change state machine

   **`port`**: Ports debug

   **`PORTS-GROUP`**: Group of Ports

   **`bdm`**: Bridge Detection state machine

   **`ppm`**: Port Protocol Migration state machine

   **`prx`**: Port Receive state machine

   **`ptx`**: Port Transmit state machine

   **`rx`**: Port MSTP receive trace

   **`sniffer`**: Port MSTP sniffer'

   **`tx`**: Port MSTP transmit trace

   **`target`**: Target of traces

   **`all`**: All targets

   **`cli`**: CLI (TELNET/SSH) sessions

   **`console`**: System console

   **`current-session`**: Current CLI session

   **`log`**: System log

***Deactivating Display***

To deactivate display of Spanning-Tree events on the CLI screen:

1. Enter **`configure terminal`** mode.
2. Invoke the command:

**no debug spanning-tree (instance <0-63> prs|root-change|port (PORTS-GROUP c|f|h|pim|prt|pst|tcm))|(port (PORTS-GROUP bdm|ppm|prx|ptx|rx|sniffer|tx))|(target (all|cli|console|current-session|log))**

## Disabling Debugging Functions

To disable debugging functions:

1. Enter **enable** mode.
2. Invoke the command:
   **undebug all|(bgp [events|filters|fsm|keepalives|nsm|updates])**
   where,
   **all**: All debugging
   **bgp**: BGP information
   **events**: BGP events
   **filters**: BGP filters
   **fsm**: BGP information
   **keepalives**: BGP keepalives
   **nsm**: NSM message
   **updates**: BGP updates

## Process-Failure File

This section normally applies to the Customer Support Officer (CSO). Before using the commands in this section, consult with CSO.

The Process-Failure File usually shows the sequence of functions that led to the OS900 system's crash.

### Configuration

#### *Creation*

By default, the OS900 does not create a process-failure file.

The process-failure file can be found on entering **linux** mode (as described in the section *Linux Mode*, page *101*) under the name **cd \config**.

Enable

To cause the OS900 to create a process failure file:

1. Enter boot mode by invoking the following sequence of commands:
   **enable → configure terminal → boot**
2. Invoke the command:
   **exception enable**

Disable

To prevent the OS900 from creating a process failure file:

1. Enter boot mode by invoking the following sequence of commands:
   **enable → configure terminal → boot**
2. Invoke the command:
   **exception disable**

#### *Size*

Custom

*Limited*

To change the size of the process failure file:

1. Enter boot mode by invoking the following sequence of commands:
   **enable → configure terminal → boot**

2. Invoke the command:
   **`exception memory <1-200>`**
   where,
   **`<1-200>`**: Range of numbers of blocks (each block of size 1-Kbyte) from which one is to be selected.

*Unlimited*

To allow the process failure file to be of any size:

1. Enter boot mode by invoke the following sequence of commands:
   **`enable → configure terminal → boot`**
2. Invoke the command:
   **`exception memory unlimited`**

Default

By default, the size of the process failure file is 300 Kbytes.
To reset the size of the process failure file to this default value (300 Kbytes):

1. Enter boot mode by invoke the following sequence of commands:
   **`enable → configure terminal → boot`**
2. Invoke the command:
   **`no exception memory`**

***Reboot***

Enable

By default, the OS900 automatically reboots if failure of a critical internal process occurs.
To cause the OS900 to reboot if such a failure occurs:

1. Enter boot mode by invoking the following sequence of commands:
   **`enable → configure terminal → boot`**
2. Invoke the command:
   **`exception behaviour reboot`**

Disable

To prevent the OS900 from rebooting when an internal process fails:

1. Enter boot mode by invoking the following sequence of commands:
   **`enable → configure terminal → boot`**
2. Invoke the command:
   **`exception behaviour halt`**

Default

To set the default mode for internal process failure, i.e., to cause the OS900 to reboot if such a failure occurs:

1. Enter boot mode by invoking the following sequence of commands:
   **`enable → configure terminal → boot`**
2. Invoke the command:
   **`no exception behaviour`**

***Saving***

To save the configuration, invoke either of the following the commands:

**`write memory`**
**`write file`**

**Activation**

Creation of a process-failure file is done off-line. Accordingly, to activate creation of the file, the OS900 must be rebooted. To reboot the OS900, invoke either of the following commands in **`enable`** mode:

**`reboot`**
**`reboot-force`**

# Counters

**Table 36: Counters**

| | | OS900 | OS940 | OS9124 |
|---|---|---|---|---|
| **Ports** | Ingress | None | None | None |
| | Egress | None | 64 counters per port, one for each of 64 combinations obtainable by selecting the police mode (drop or pass), the SL (1 to 8), the color (red or green), and the data unit size (packet or byte).<br>A byte counter is 35 bits in size and can count 32G bytes.<br>A packet counter is 29 bits in size and can count up to 512M packets. | 64 counters per port, one for each of 64 combinations obtainable by selecting the police mode (drop or pass), the SL (1 to 8), the color (red or green), and the data unit size (byte or packet).<br>A byte counter is 35 bits in size and can count 32G bytes.<br>A packet counter is 29 bits in size and can count up to 512M packets. |
| **Inband VLAN Interfaces** | Ingress | None | None | 8K counters.<br>4K byte counters, each 35 bits in size and can count 32G bytes.<br>4K packet counter, each 29 bits in size and can count up to 512M packets.<br>A byte counter and a packet counter is assigned to each VLAN. |
| | Egress | None | None | 8K counters.<br>4K byte counters, each 35 bits in size and can count 32G bytes.<br>4K packet counter, each 29 bits in size and can count up to 512M packets.<br>A byte counter and a packet counter is assigned to each VLAN. |

**Table 36: Counters** (Cont'd)

| | | | | |
|---|---|---|---|---|
| **ACL Rules** | Ingress | 32 packet counters, each 32 bits in size.<br>Each counter may be assigned to several rules and several counters may be assigned to the same rule. | 2K counters.<br>1K byte counters, each 35 bits in size and can count 32G bytes.<br>1K packet counter, each 29 bits in size and can count up to 512M packets. | 4K counters.<br>2K byte counters, each 35 bits in size and can count 32G bytes.<br>2K packet counter, each 29 bits in size and can count up to 512M packets. |
| | Egress | | None | 4K counters.<br>2K byte counters, each 35 bits in size and can count 32G bytes.<br>2K packet counter, each 29 bits in size and can count up to 512M packets. |
| **EQM** | Ingress | 2 sets of counters.<br>Each set consists of 4 counters (Received packets, Dropped packets due to VLAN filtering, Dropped packets due to security screening, Dropped packets for other | None | None |

| | | | | |
|---|---|---|---|---|
| | | reasons) | | |
| | Egress | 2 sets of counters.<br>Each set consists of 4 counters (Unicast packets, Multicast + Unknown packets, Broadcast packets, Tx congestion packets) | Two sets of counters 'set1' and 'set2'.<br>Each set consists of eight 32-bit counters, one for each of the following packet type: Unicast, Multicast, Broadcast, Filtered egress, Tail drop, CPU + mirrored, Dropped, and Dropped multicast. | Two 32-bit counters, one for green and yellow packet, the other for red packets. |
| **TC** | Ingress | 32 byte counters, 16 for green packets and 16 for red packets.<br>Each counter is 32 bits in size. | Counters for all TCs<br>3 global counter sets.<br>Each set consists of six 32-bit counters, 2 for each of 3 colors (green, yellow, red), one for byte and the other for packet.<br>Counters per TC<br>Three 32-bit byte counters for the 3 colors (green, yellow, red). | Counters for all TCs<br>3 global counter sets.<br>Each set consists of six 32-bit counters, 2 for each of 3 colors (green, yellow, red), one for byte and the other for packet.<br>Counters per TC<br>Three 32-bit byte counters for the 3 colors (green, yellow, red). |
| | Egress | – | – | – |

# **Appendix B:** Cable Wiring

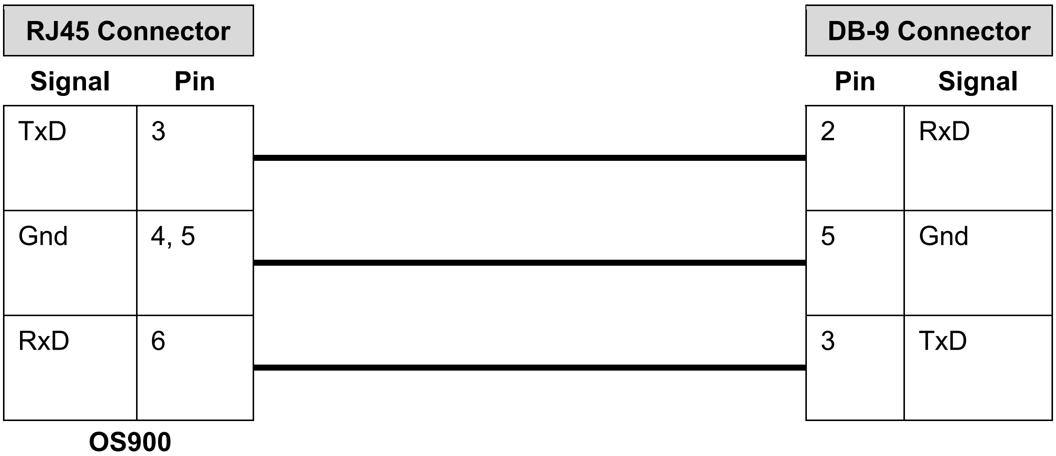



**Figure 77: Null-Modem RS-232 Cable Wiring**


**Figure 78: Ethernet *Straight* Cable Wiring**

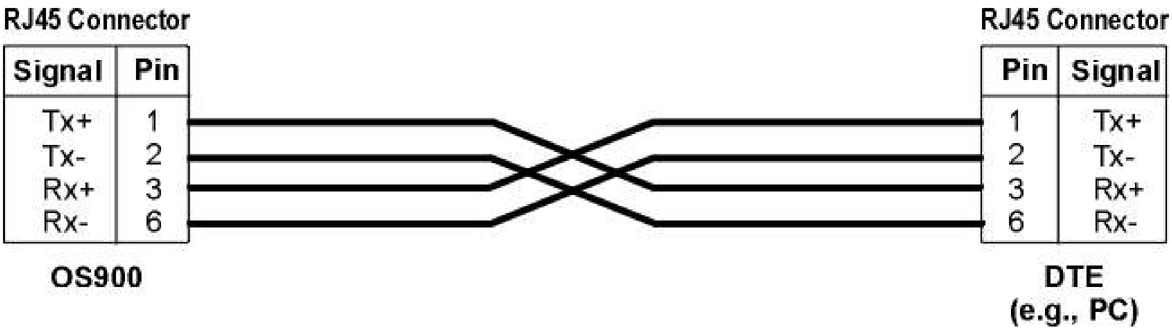



**Figure 79: Ethernet *Cross* Cable Wiring**

# **Appendix C:** Cleaning Optical Connectors

## General

Intrusions (e.g., dust, grease, etc.) at the interface of two optical fibers, such as at a pair of coupled connectors, attenuate the signal through the fiber. Consequently, optical connectors must be clean before they are coupled with other connectors.

## Tools and Equipment

Following are tools and equipment required for cleaning connectors.

- **Dust caps**
  Caps for protecting the connector from intrusions. A cap is usually made from flexible plastic. When placing a cap over a connector, avoid pressing it against the fiber ferula surface in the connector so as to prevent contamination.
- **Isopropyl alcohol**
  Solvent for contaminants.
- **Tissues**
  Soft multi-layered fabric made from non-recycled cellulose.

## Procedure

The procedure for cleaning connectors is as follows:

1. If no stains are present, using a new clean dry tissue, gently rub, in small circular motions, the exposed fiber surface and surrounding area in the connector to remove dust.
2. If stains are present, moisten a new clean dry tissue with isopropyl alcohol and gently rub, in small circular motions, the exposed fiber surface and surrounding area in the connector to remove the stains.
3. Using a new clean *dry* tissue, gently rub, in small circular motions, the exposed fiber surface and surrounding area in the connector to remove the dissolved stains and excess isopropyl alcohol.
4. If a connector is not to be coupled with another immediately, cover it with a dust cap.

# Appendix D: Troubleshooting

The troubleshooting procedure here is on the operative level and is given in *Table 37*, below. Read the entries in the column **Problem** until you reach the problem that applies to the OS900. Then perform the corrective action(s) appearing in the same row. If the problem persists, note the status of all the LEDs and consult your *MRV* representative.

**Table 37: Startup and Operation Troubleshooting**

| Row | Problem | Probable Cause | Corrective Action |
|---|---|---|---|
| 1 | LED **PWR** ON-Amber | Power into the OS900 system was shutdown due to continuous pressing of Pushbutton **PWR** for at least 2 seconds. | 1. Press Pushbutton **PWR** continuously for at least 2 seconds. |
| 2 | LED **PWR** OFF | No power at the entrance to the OS900 system from a Power Supply. | 1. Ensure that the power cord is securely connected to the power source output and to the Power Supply in the OS900.<br>2. Ensure that power is present at the power source output.<br>3. Ensure that the power cord of Power Supply is not damaged. |
| 3 | LED **TMP** ON-Amber | Insufficient cooling air. | 1. Verify that no obstacles to cooling air flow are present around the OS900.<br>2. Verify that the fan is running. |
| 4 | LED **TMP** OFF | No power into the OS900 system. | 1. Ensure that the actions in Rows 1 to 3, above, have been performed. |
| 5 | LED **TR** OFF | Management station not connected. | Perform PING. If there is no response from the management station, do the following:<br>1. Verify that connection of the OS900 to the Ethernet LAN, to which the management station is connected, is OK.<br>2. Management station is connected to the Ethernet LAN.<br>3. The management station is correctly setup and operational.<br>4. If the management station is a craft terminal, set the baud rate for the craft terminal to 9600 baud.<br>5. Verify that the network exists in the routing table.<br>6. Check the default gateway.<br>7. Flush the ARP table with the CLI command (since the ARP table may contain outdated information). |

**Table 37: Startup and Operation Troubleshooting**

<table>
<tr><th>Row</th><th>Problem</th><th>Probable Cause</th><th>Corrective Action</th></tr>
<tr><td>6</td><td>L LED OFF</td><td>No Ethernet link integrity signal being received.</td><td>Electrical Port (10/100/1000Base-T Port):<br>1. Verify that the cable connecting the OS900 port to the network is securely connected at both ends and is undamaged.<br>2. Enter <code>configure terminal</code> mode and enable the port using the following CLI command:<br><code>port state enable</code><br>3. If the port is connected to a DTE (e.g., PC, workstation, etc.), make sure the DTE is powered on and the NIC is OK. (The NIC can be checked by running a diagnostic test with the software supplied by the vendor.)<br>4. Temporarily attach the cable to another OS900 port to determine whether the port is faulty.<br>Fiberoptic Port (100/1000Base-X Port:<br>1. For each cable fiber, ensure Tx ←→ Rx interconnection.<br>2. Verify that the cable connecting the OS900 port to the network is securely connected at both ends and is undamaged.<br>3. Enter <code>configure terminal</code> mode and enable the port using the following CLI command:<br><code>port state enable</code><br>4. Clean the fiberoptic connectors of the cable and OS900 port as described in Appendix C: Cleaning Optical Connectors, page 807.<br>5. Ensure that the cable type (singlemode or multimode) is right and the attenuation and length are such that the power budget is not exceeded.<br>6. Temporarily attach the cable to another OS900 port to determine whether the port is faulty.</td></tr>
<tr><td>7</td><td>A LED OFF</td><td>DTE(s) not transmitting to/via port.</td><td>1. Ensure that L LED is on, possibly by performing the actions described in row 7.<br>2. Make sure the DTE(s) are powered on.</td></tr>
<tr><td>8</td><td>No manageme nt access</td><td>Access restricted to administrator password</td><td>1. Verify correctness of user name and password, including case of letters.<br>2. Enter <code>admin</code> for username.</td></tr>
</table>

# Appendix E: Packet Processing Stages

## Ingress

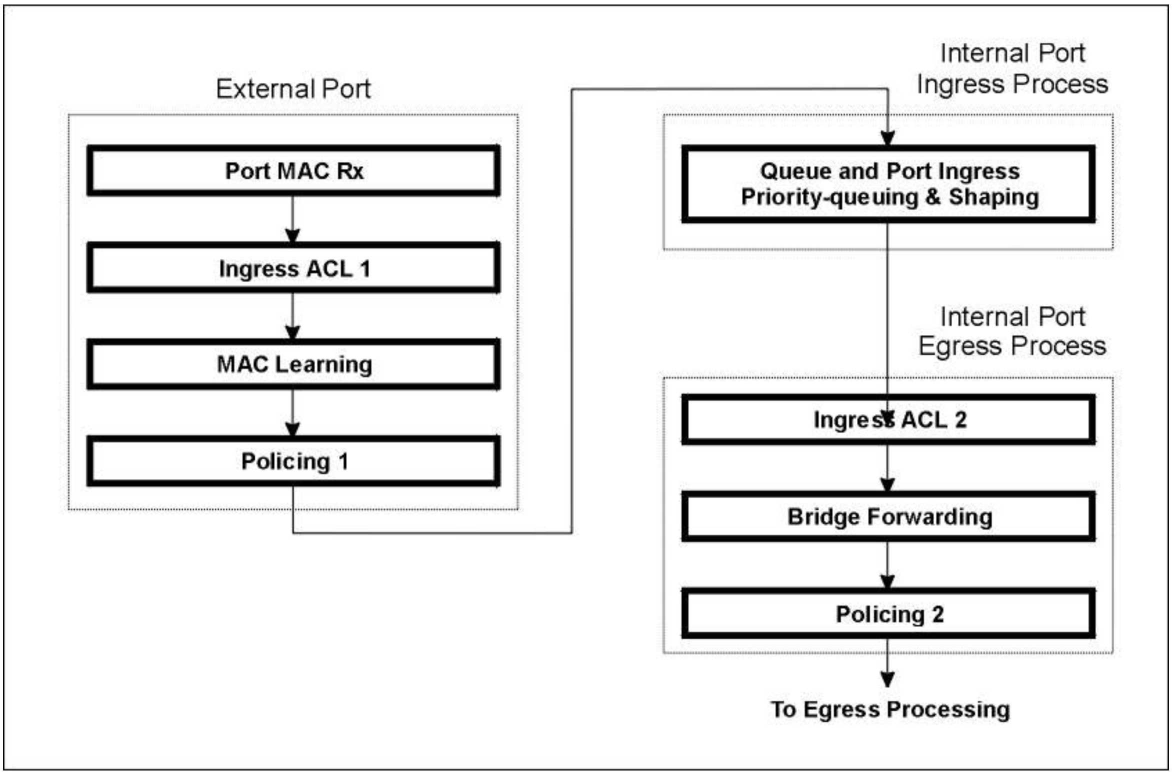



**Figure 80: Ingress Packet Processing Stages**

## Egress

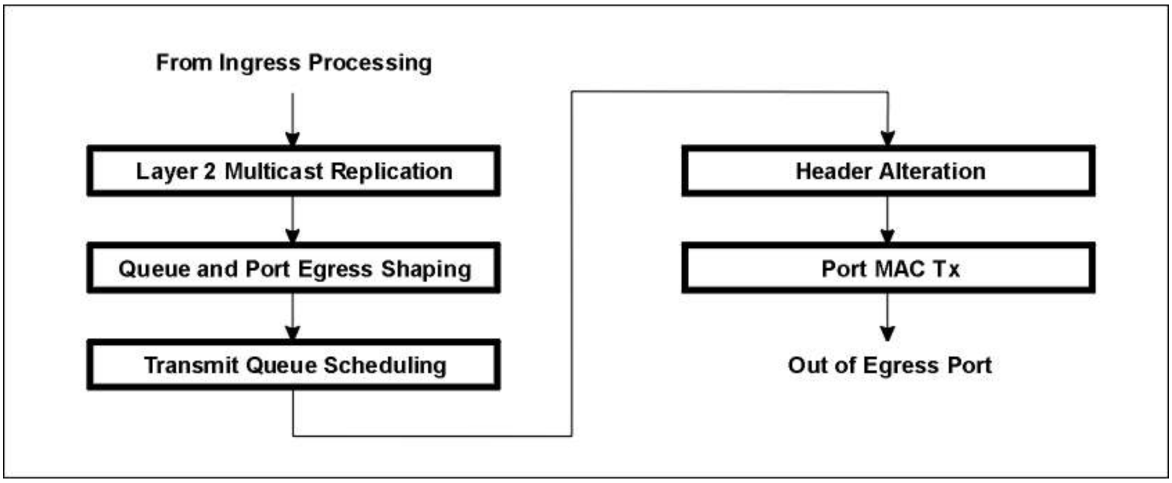



**Figure 81: Egress Packet Processing Stages**

Ingress ACL 1 is for ACLs bound using `access-group` within a VLAN interface or to a port using `port access-group [PORT]`.
Policing 1 is for TC actions in ACLs from 'Ingress ACL 1'.

Ingress ACL 2 is for ACLs bound to a port as a second ACL using **`port access-group extra [PORT]`**.
Policing 2 is for TC actions in ACLs from 'Ingress ACL 2'.

# Appendix F: Product Specification

| Services and Interfaces | OS904 | OS906 | OS910 | OS912 |
|---|---|---|---|---|
| MEF Services and Certifications | EPL, E-Line, E-LAN, E-Tree, MEF 9, 14, 21 | EPL, E-Line, E-LAN, E-Tree, MEF 9, 14, 21 | EPL, E-Line, E-LAN, E-Tree, MEF 9, 14, 21 | EPL, E-Line, E-LAN, E-Tree, MEF 9, 14, 21 |
| Non-blocking architecture<br>Wire-speed forwarding | ✓ | ✓ | ✓ | ✓ |
| All ports can serve as UNI/ENNI | ✓ | ✓ | ✓ | ✓ |
| 10/100/1000Base-T | | | 8 | |
| 10/100/1000Base-T or 100/1000Base-X SFP | 2 | 6 | | 12 |
| 100/1000Base-X SFP | 2 | | 2 | |
| Hot-swappable SFP/XFP Optics | Short/Long-haul, Multi-rate, BX & WDM | Short/Long-haul, Multi-rate, BX & WDM | Short/Long-haul, Multi-rate, BX & WDM | Short/Long-haul, Multi-rate, BX & WDM |
| Power Supply (AC = A, DC = D, 2 = redundancy) | A, D | A, D, 2A, 2D | A, D, 2A, 2D | 2A, 2D |
| **Hardware** | | | | |
| 10/100/1000Base-T ports | Auto-MDI/MDIX | | | |
| Learn Table | MAC, Up to 16K entries capacity, Limitable per VLAN/port | | | |
| FIB Size | 4K entries | | | |
| Jumbo Frame Lengths Supported (max) | Up to 16K bytes, on all ports | | | |
| Packet Buffer | Automatically managed | | | |
| Environmental-Temperature Sensor | Built-in | | | |
| **Operation** | | | | |
| Performance | Non-blocking, wire-speed on all ports | | | |
| MTBF: | | | | |
| OS904/AC-1 | 283,000 hr @ 25 °C (77 °F) | | | |
| OS904/DC-1 | 459,892 hr @ 25 °C (77 °F) | | | |
| OS904E/AC-1 | 39,070 hr @ 65 °C (149 °F) | | | |
| OS904E/DC-1 | 105,549 hr @ 65 °C (149 °F) | | | |
| OS904EXT/AC-1 | 14,073 hr @ 65 °C (149 °F) | | | |
| OS904EXT/DC-1 | 81,255 hr @ 65 °C (149 °F) | | | |

| **Operation** (Cont'd) | |
|---|---|
| OS904EXT/AC-1N | 14,073 hr @ 65 °C (149 °F) |
| OS906/AC-1 | 161,021 hr @ 25 °C (77 °F) |
| OS906/DC-1 | 386,477 hr @ 25 °C (77 °F) |
| OS906/AC-2 | 237,510 hr @ 25 °C (77 °F) |
| OS906/DC-2 | 407,513 hr @ 25 °C (77 °F) |
| OS910/AC-1 | 220,733 hr @ 25 °C (77 °F) |
| OS910/DC-1 | 463,503 hr @ 25 °C (77 °F) |
| OS910/AC-2 | 257,000 hr @ 25 °C (77 °F) |
| OS910/DC-2 | 505,749 hr @ 25 °C (77 °F) |
| OS910-M | 240,353 hr @ 25 °C (77 °F) |
| OS912-AC-2 | 252,266 hr @ 25 °C (77 °F) |
| OS912-DC-2 | 311,756 hr @ 25 °C (77 °F) |
| OS930/AC-2 | 540,353 hr @ 25 °C (77 °F) |
| **Switching Services** | |
| IEEE 802.1Q and IEEE802.1ad provider bridges: | 4K active VLANs (max)<br>Q-in-Q stacking (per port/VLAN)<br>VLAN translation and mapped modes (per port/VLAN) |
| Layer 2 Control Protocol Tunneling | BPDU, CDP, VTP, PVST+, etc. |
| Media Cross Connect™[105] | Software-controlled, transparent, no MAC address learning |
| Multicast Services | IGMP v1 and v2, IGMP snooping (IPv4 and IPv6 MLD snooping), Multicast join lists per port/VLAN (1k multicast groups per system), Static multicast range set |
| Protection | Automatic Optical switching on network interfaces (1:1)<br>IEEE802.3ad Link Aggregation (1 + 1)<br>IEEE 802.1s Multiple Instance STP with compatibility to IEEE 802.1w and IEEE 802.1d STPs<br>Loop prevention at ports without the use of STP<br>Link flap guard, Port protection, BPDU storm guard |
| **Traffic Management Services (MEF Compliant)** | |
| Inbound & Outbound traffic | Per flow management |
| Classification | By physical port, MAC, Ethertype, VLAN, IP/TCP/UDP, IEEE 802.1p VPT, DiffServ (IPv4 & IPv6 TC), MPLS label EXP bits |
| QoS Marking/remarking | Per Service Level according to L2 IEEE 802.1p VPT, MPLS L2+ EXP, L3 DSCP, or MPLS EXP |
| CoS | 8 hardware queues per port & configurable CoS adaptive buffer |
| In-profile and out-of-profile service counter sets | per UNI, CoS, EVC |
| Class-aware rate limit | Dynamic bandwidth reuse between mapped classes, Hierarchical-QoS model with CIR/CBS metering |

[105] An MRV advanced patch-panel function technology

| **Tunneling Layer 2 Services** | |
|---|---|
| Q-in-Q | Mapped mode or translation |
| Layer 2 VPN | Martini MPLS pseudo-wire |
| MPLS VC | For direct connection into MPLS domains or H-VPLS MTU-s. |
| **IP Services** | |
| IGP and EGP routing using Master-OS™ | |
| DHCP Server/Client (using BOOTP)/Relay/DHCP Option 82 | |
| **Security** | |
| CPU DoS protection (Frame rate control, Dedicated queues) | |
| Wire-speed Access Control Lists (L2-3-4: from frame to application layer) | |
| MAC, ARP, and BPDU filtering | |
| Rate limit protection for Unicast/Multicast/Broadcast packets | |
| IEEE 802.1x* | |
| Software-based NAT/NAPT & Stateful Firewall* | |
| Security thresholds for L2 statistics counters | |
| Filtering rules for control protocols (e.g., BPDU, CDP, VTP, PVST+, etc.) without the need for ACLs or STP operation for BPDUs blocking | |
| **Management & Diagnostics Tools** | |
| Industry Standard CLI | |
| Out-of-band Ethernet management – EIA-232 console | |
| Out-of-band Ethernet management – Dedicated Ethernet RJ45 port | |
| TELNET, SSH v2, SNMPv3, RMON (4 groups), Secure Copy | |
| View-based Access Control Model (VACM) | |
| Port mirroring - ingress and egress traffic to analyzer port | |
| Remote mirroring per ACL (port/service/flow) to analyzer VLAN | |
| PING, Traceroute, DNS lookup, TCP dump (built-in LAN analyzer) | |
| Management ACL for trusted connections (TELNET, SSH, SNMP) | |
| Option to block SNMP/CLI access | |
| Hierarchical Administration policy | |
| RADIUS and TACACS+ Authentication, Authorization, and Accounting (AAA)for management sessions | |
| Configuration load/save via FTP and Secure Copy (SCP) | |
| Network Time Protocol (NTP) | |
| Logging Syslog (Local and Remote) | |

| **Management & Diagnostics Tools** (Cont'd) |
|---|
| Scripting tool for macro configurations and maintenance |
| Scheduler for execution of administrator-specified commands at administrator-preset times |
| Save mode for multiple configuration files |
| Extended statistics per port on a trunk |
| Show mode extensions (partition version/number/size) |
| BOOTP extensions (broadcast, timeout, out-of-band Ethernet interface option) |
| Bridging function for out-of-band Ethernet interface |
| **OAM - Service Assurance Tools** |
| Enhanced performance monitoring and SLA management<br>- Local and Remote hardware-based loopback functionality<br>- Per-VLAN loopback & MAC swapping<br>- Enhanced Latency/Jitter measurement (QoS Verification)<br>- Alarming control |
| End-to-end service OAM<br>- Connectivity Fault Management – IEEE 802.1ag (MEP/MIP)<br>- Performance Measurement ITU Y.1731 (latency, jitter, and loss with microsecond accuracy)<br>- RFC 2544 Internal Traffic Generator for measuring and reporting performance characteristics for throughput rates of up to 1 GigabitE<br>- Generation of synthetic traffic with rates of up to 1 GE based on Y.1731<br>- Private MIB extending Y.1731 (last result table and CCM fault/clear trap)<br>- Response Time Reporter for IP services<br>- IEEE 802.3ah OAM for Ethernet in the First Mile (EFM): Auto discovery, Dying gasp, SNMP trap, and Loopback<br>- Discovery Link Fault/Critical Dying Gasp<br>- Physical Layer OAM (Virtual Cable Diagnostics)<br>  ▪ Optical signal level monitoring (for SFP SFF-8472)<br>  ▪ Copper TDR on 10/100/1000Base-T ports<br>- Remote failure notification<br>  ▪ Link-Integrity Notification (LIN)<br>  ▪ Dying Gasp<br>- OAM CCM binding for service protection |

| **Power Consumption (Max)** | |
|---|---|
| OS904/AC-1 | 100-240 Vac, 50-60 Hz, 0.16/0.08 A (15 W or 51 Btu/hr) |
| OS904/DC-1 | -48/60 Vdc, 0.5 A (15 W or 51 Btu/hr) |
| OS904EXT/DC-1 | -48/60 Vdc, 3.5 A (125 W or 425 Btu/hr) |
| OS906/AC-1 | 100-240 Vac, 50-60 Hz, 0.26/0.13 A (30 W or 102 Btu/hr) |
| OS906/AC-2 | 100-240 Vac, 50-60 Hz, 0.3/0.15 A (36 W or 123 Btu/hr) |
| OS906/DC-1 | -48/60 Vdc, 0.8 A (30 W or 102 Btu/hr) |
| OS906/DC-2 | -48/60 Vdc, 1.0 A (36 W or 123 Btu/hr) |
| OS910/AC-1 | 100-240 Vac, 50-60 Hz, 0.25/0.12 A (25 W or 85 Btu/hr) |
| OS910/AC-2 | 100-240 Vac, 50-60 Hz, 0.3/0.15 A (30 W or 102 Btu/hr) |

| **Power Consumption (Max)** (Cont'd) | |
|---|---|
| OS910/DC-1 | -48/60 Vdc, 0.69 A (25 W or 85 Btu/hr) |
| OS910/DC-2 | -48/60 Vdc, 0.83 A (30 W or 102 Btu/hr) |
| OS910-M | AC: 100-240 Vac, 50-60 Hz, 0.6/0.3 A<br>DC: -48/60 Vdc, 1.5 A |
| Basic | 51 W or 174 Btu/hr |
| 4 x SFPs | 2 W or 6.8 Btu/hr |
| 2 x EM9-CES-4E1C Modules | 16 W or 54.5 Btu/hr |
| OS912-AC-2 | 100-240 Vac, 50-60 Hz, 0.48/0.24 A (49 W or 167 Btu/hr) |
| OS912-DC-2 | -48/60 Vdc, 1.5 A (49 W or 167 Btu/hr) |
| OS930 | AC: 100-240 Vac, 50-60 Hz, 1.0/0.5 A (Max: 115 W or 393 Btu/hr)<br>DC: -48/60 Vdc, 2.5 A (Max: 115 W or 393 Btu/hr) |
| **Ports** | |
| 10/100/1000Base-T: | |
| Interface | Fixed |
| Purpose | Connection to Ethernet/Fast Ethernet/Gigabit Ethernet DTE or DCE |
| Number | |
| OS904 | 2 |
| OS906 | 6 |
| OS910 | 8 |
| OS910-M | 8 |
| OS912 | 12 |
| OS930 | – |
| Connector: | |
| *Type* | RJ45, female, 8-pin, shielded |
| *Pinout* | Auto-MDI/MDIX, i.e., each port can be connected to an Ethernet MDI (Pinout: 1 → Tx+, 2 → Tx-, 3 → Rx+, 6 → Rx-) or MDIX (Pinout : 1 → Rx+, 2 → Rx-, 3 → Tx+, 6 → Tx-) port with a straight or cross-over cable since the port automatically configures itself to suit the cable type and co-port interface. |
| Cabling: | |
| *Length (max)* | 100 m (~ 330 ft) |
| *Type* | Category 5 |
| *Connector* | RJ45,, male, 8-pin, shielded |
| 100/1000Base-X: | |
| Interface | Hot-swappable SFP |
| Purpose | Connection to uplink Fast Ethernet/Gigabit Ethernet DTE or DCE |

| **Ports** (Cont'd) | |
|---|---|
| Number (max) | |
| OS904 | 4 |
| OS906 | 6 |
| OS910 | 2 (Ports 9 and 10) |
| OS910-M | 2 (Ports 9 and 10) |
| OS912 | 12 |
| OS930 | – |
| Connector Type: | Dual, female, LC (usually) |
| Cabling: | |
| *Length (max)* | Per the SFP |
| *Type* | Per the SFP |
| *Connector* | Dual, male, LC (usually) |
| 10 Gbps Ethernet: | |
| Interface | Hot-swappable XFP |
| Purpose | Connection to uplink 10 Gbps Ethernet DTE or DCE |
| Number (max) | |
| OS930 | 3 |
| Connector Type: | Dual, female, LC (usually) |
| Cabling: | |
| *Length (max)* | Per the XFP |
| *Type* | Per the XFP |
| *Connector* | Dual, male, LC (usually) |
| Management Console (Serial over RS-232) – **CONSOLE EIA-232**: | |
| Purpose | Craft terminal (ASCII, e.g., VT100) connection |
| Number | 1 |
| Connector: | |
| *Type* | RJ45, female, 8-pin |
| *Pinout* | 3→TxD; 4→Gnd; 5→Gnd; 6→RxD (Pins 1, 2, 7, and 8 not used) |
| Cabling: | |
| *Length* | 15 m (~ 50 ft) |
| *Connector* | RJ45, male, 8-pin |

| **Ports** (Cont'd) | |
|---|---|
| Management via 10/100Base-TX Ethernet – **MGT ETH**: | |
| Purpose | NMS connection |
| Number | 1 |
| Connector: | |
| *Type* | RJ45, female, 8-pin |
| *Pinout* | MDI (1 ←→ Tx+; 2 ←→ Tx-; 3 ←→ Rx+; 6 ←→ Rx-) |
| Cabling: | |
| *Length* | Up to 100 m (328 ft) |
| *Type* | Category 5, Cross-wired (as shown in *Figure 79*, page *805* ) |
| *Connector* | RJ45, male, 8-pin |
| **LEDs** | |
| Global Status | **PWR** – System power; **RST** or **PRP** – Reset; **TMP** or **TEMP** – Temperature, **PS1** – Power Supply 1 power, **PS2** – Power Supply 2 power, **FAN** – Internal fans status |
| Port Status | **L&A** – Link integrity/Activity, **L** – Link integrity, **A** – Link Activity |
| **Pushbuttons** | |
| Power | **PWR** – used to power ON/OFF the OS900 |
| Reset | **RST** – used to reset the OS900 |
| **Environmental** | |
| Temperature[106]: | |
| Testing Standard | ETSI EN300-019, Class 3.1 |
| Operating | |
| Regular | 0 to 50 °C (32 to 122 °F) |
| Extreme | |
| OS904E/AC-1, OS904E/DC-1 | -10 to 65 °C (14 to 149 °F) |
| OS904EXT/AC-1, OS904EXT/AC-1N, OS904EXT/DC-1 | -40 to 65 °C (-40 to 149 °F) |

[106] In even more extreme weather conditions (e.g., UV radiation, rain, dust, humidity, corrosion, etc.), OS900s can be housed in *MRV*'s weather-proof Outdoor Cabinets.

| **Environmental** (Cont'd) | |
|---|---|
| Storage | |
| Regular | -25 to +70 °C (-13 to 158 °F) |
| Extreme | |
| OS904E/AC-1, OS904E/DC-1 | -35 to +85 °C (-31 to 185 °F) |
| OS904EXT/AC-1, OS904EXT/AC-1N, OS904EXT/DC-1 | -75 to +85 °C (-133 to 185 °F) |
| Humidity (non-condensing) | 10 to 85% |
| Dust | Less than $10^6$ particles/$m^3$ (~ 30,000 particles/$ft^3$) |
| **Physical** | |
| Dimensions (W x H x D): | |
| OS904/AC-1, OS904/DC-1 | 219.6 x 43.65 x 265 mm $^3$ [8.64 x 1.72 x 10.43 in $^3$] |
| OS906/AC-1, OS906/DC-1 | 219.6 x 43.65 x 265 mm $^3$ [8.64 x 172 x 10.43 in $^3$] |
| OS906/AC-2, OS906/DC-2 | 443 x 43.65 x 204 mm $^3$ [17.4 x 1.72 x 8.03 in $^3$] |
| OS910/AC-1, OS910/DC-1, OS910/DC-2 | 214.6 x 43.65 x 240 mm $^3$ [8.45 x 1.72 x 9.45 in $^3$] |
| OS910/AC-2 | 443 x 43.65 x 204 mm $^3$ [17.4 x 1.72 x 8.03 in $^3$] |
| OS910-M | 443 x 43.65 x 315 mm $^3$ [17.44 x 1.72 x 12.4 in $^3$] |
| OS912-AC-2, OS912-DC-2 | 443 x 43.65 x 204 mm $^3$ [17.4 x 1.72 x 8.03 in $^3$] |
| OS930 | 444 x 43.65 x 290 mm $^3$ [17.48 x 1.72 x 11.4 in $^3$] |
| Weight (max): | |
| OS904/AC-1: | |
| Without PS | 1.1 kg ( lb) |
| With PS | 1.85 kg ( lb) |
| OS904/DC-1: | |
| Without PS | 1.05 kg ( lb) |
| With PS | 2.25 kg ( lb) |
| OS904E/AC-1: | |
| Without PS | 1.25 kg ( lb) |
| With PS | 2.25 kg ( lb) |
| OS906/AC-1: | |
| Without PS | 1.35 kg ( lb) |

| **Physical** (Cont'd) | |
|---|---|
| With 1 PS | 2.0 kg (2.87 lb) |
| OS906/DC-1: | |
| Without PS | 1.3 kg ( lb) |
| With PS | 2.1 kg (2.87 lb) |
| OS906/AC-2: | |
| Without PS | 1.95 kg ( lb) |
| With PS | 3.5 kg (2.87 lb) |
| OS906/DC-2: | |
| Without PS | 1.95 kg ( lb) |
| With PS | 2.95 kg (2.87 lb) |
| OS910-M: | |
| Without PS | 2.45 kg (5.39 lb) |
| With 1 PS | 2.76 kg (6.07 lb) |
| With 2 PS | 3.06 kg (6. 73 lb) |
| OS912/AC-2: | |
| Without PS | 2.0 kg ( lb) |
| With PS | 3.5 kg (2.87 lb) |
| OS912/DC-2: | |
| Without PS | 2.0 kg ( lb) |
| With PS | 3.5 kg (2.87 lb) |
| OS930: | |
| Without PS | 2.61 kg |
| With 1 PS | 3.4 (7.5 lb) |
| With 2 PS | 4.19 (9.22 lb) |
| Mounting | Desktop, wall, or 19-inch (482.6 mm) or 23-inch (584.2 mm) rack per the ETSI 300-019 standard, class 3.1. No clearances required between units. |
| **Management** | |
| Web-Based | Using MegaVision ® management application or MIB Browser |
| SNMP | Using MegaVision ® management application or any other SNMP manager |
| TELNET | Using a TELNET station |
| Serial/RS-232 | Using craft terminal (e.g., VT100 Terminal or PC with ASCII terminal/emulator software) |
| IP Address Management | DHCP |

| | |
|---|---|
| **Accessories** | |
| Rack-Mount | Two brackets for mounting in a 19-inch or 23-inch rack |
| **Counters** | |
| Port | |
| Ingress | None |
| Egress | None |
| Interface (VLAN) | |
| Ingress | None |
| Egress | None |
| ACL Rules | 32 packet counters, each 32-bit of size for ACLs bound to ingress or egress ports. A counter may be assigned to several rules or several counters may be assigned to a rule. |
| EQM | |
| Ingress | 2 sets. Each set has 4 counters for Receive packet, Drop due to VLAN filter, Drop due to security, and Drop for other reason. |
| Egress | 2 sets. Each set has 4 counters for ucast, mcast + unknown, bcast, Tx congestion. |
| TC | 32 byte counters, 16 for green packets and 16 for red packets |
| **Compliance** | |
| Safety | Designed to comply with IEC 60950-1:2005 (2nd Edition) and EN 60950-1:2006; UL 60950-1:2nd Edition; CSA C22.2 No. 60950-1:2nd Edition; FCC Part 15, Class B; 2004/108/EC, 2006/95/EC, RoHS.<br>Class I laser products. Internal lasers comply with IEC 60 825-1:1993 + A1:1997 + A2:2001/EN60825-1:1994 + A1:1996 + A2:2001. |
| Operation | |
| IETF | UDP – RFC 768<br>TFTP – RFC 783<br>IP – RFC 791<br>ICMP – RFC 792<br>TCP – RFC 793<br>ARP – RFC 826<br>Multi-session TELNET – RFC 854<br>Transmission of IP Datagrams over Ethernet Networks – RFC 894<br>FTP – RFC 959<br>IGMPv1 – RFC 1112<br>Host Requirements – RFC 1122<br>Structure and Identification of Management Information for TCP/IP-based Internets – RFC 1155<br>SNMP v1 – RFC 1157<br>Concise MIB Definitions – RFC 1212<br>MIB II (all objects) – RFC 1213<br>Trap Convention – RFC 1215<br>Ethernet-like statistics MIB – RFC 1284<br>The MD5 Message-digest Algorithm – RFC 1321<br>CIDR – RFC 1519<br>DNS client – RFC 1591 |

| | |
|---|---|
| | Ethernet MIB – RFC 1643<br>per-port RMON IEEE 802.1: Ethernet statistics (Group 1), History (Group 2), Alarm (Group 3), and Event (Group 9) – RFC 1757<br>Structure of Management Information for SNMPv2 – RFC 1902<br>SNMPv2 – RFC 1907<br>IP MIB – RFC 2011<br>TCP MIB – RFC 2012<br>UDP MIB – RFC 2013<br>SNTP – RFC 2030<br>Entity MIB – RFC 2037<br>BootP and DHCP Relay (UDP Relay) – RFC 2131<br>IGMP v2 – RFC 2236<br>Network Ingress Filtering – RFC 2267<br>Opaque LSA support – RFC 2370<br>MD5 peer password authentication – RFC 2385<br>A Provider architecture for DiffServ and TE – RFC 2430<br>DiffServ of DS field in IPv4 & IPv6 headers – RFC 2475<br>SNMPv3 – RFC 2571, 2572, 2573, 2574, 2575<br>Assured Forwarding DiffServ PHB Group – RFC 2597 |
| **Compliance** (Cont'd) | |
| IETF (Cont'd) | Expedited Forwarding DiffServ PHB Group – RFC 2598<br>Definitions of Managed Objects for the Ethernet-like Interface Types – RFC 2665<br>VRRP MIB (All objects except VRRP Router Statistics (vrrpRouterChecksumErrors, vrrpRouterVersionErrors, vrrpRouterVrIdErrors, and vrrpRouterStatsTable) and Trap Definitions) – RFC 2787<br>RMON MIB – RFC 2819<br>The Interfaces Group MIB – RFC 2863<br>RADIUS Authentication – RFC 2865<br>RADIUS Accounting – RFC 2866<br>Management SLA MIB – RFC 2925 (Only for IP SLA)<br>DiffServ PHB identification codes – RFC 3140<br>BSD Syslog – RFC 3164<br>AF-PHB Group – RFC 3246<br>IGMP Ver. 3 – RFC 3376<br>SNMP version 3 Framework – RFC 3410<br>An Architecture for Describing SNMP Management Frameworks – RFC 3411<br>Message Processing and Dispatching for SNMP – RFC 3412<br>SNMP Applications – RFC 3413<br>User-based Security Model (USM) for SNMPv3 – RFC 3414<br>View-based Access Control Model (VACM0 for SNMP – RFC 3415<br>Version 2 of the Protocol Operations for SNMP – RFC 3416<br>Management Information Base (MIB) for SNMP – RFC 3418<br>OSPF (All read-only objects except ospfRouteGroup, Address range Table, OSPF Host Table, Conformance information) – RFC 1850<br>RIPv2 (All read-only objects in the RIP Interface *Status* table (rip2IfStatTable, RIP Interface *Configuration* Table (rip2IfConfTable), and Peer Table (rip2PeerTable) – RFC 1724<br>BGP4 – RFC 1657 |
| Private MIBs | Dev-cfg NbDevRouterSaveConfig. |

| | | |
|---|---|---|
| | | Objects in the Device's Power Supplies Group (NbsDevPS) |
| | Gswitch1 | All objects (read-only) |
| | Nstack | Objects in the Stack Information Group (nbsStackSlotCapacity, nbsStackSlotsTableSize, nbsStackPortsCapacity, nbsStackSlotPortsCapacity)<br>Objects in the Slot Information Group (nbsStackSlotTable) |
| | rt-cfg | All objects except Objects in the Device Virtual Interface Table (old) |
| | Switch1 | All objects except nbSysSnmpCfg, nbSysTrapEntry. |
| | OaSwitch | All objects |
| | Tcgroup | All objects |
| | OaDhcp | All objects |
| | OaSlStat | All objects |
| | nbEthOam.mib | All objects.<br>(Private extension of the DOT1AG.MIB). |
| **Compliance** (Cont'd) | | |
| ITU | ITU-T Y.1307.1 – Ethernet Private Line Service<br>ITU-T WDM grid – Optical Service<br>ITU-T grid (G.694.2) – Wavelengths with 20 nm spacing for CWDM<br>ITU-T grid (G.694.1) – Wavelengths with 100 GHz or 200 GHz spacing for DWDM | |
| IEEE | IEEE 802.3 Ethernet<br>IEEE 802.3u Fast Ethernet<br>IEEE 802.3z Gigabit Ethernet (1000Base-SX/LX)<br>IEEE 802.3ae 10 Gigabit Ethernet<br>IEEE 802.3ab Gigabit Ethernet Copper<br>IEEE 802.3ad Link Aggregation<br>IEEE 802.3ah Ethernet in the First Mile<br>IEEE 802.1D Bridging and Spanning Tree<br>IEEE 802.1p Layer 2 priority QoS Support<br>IEEE 802.1Q VLAN Tagging<br>IEEE 802.1w Rapid STP<br>IEEE 802.1s Multiple-instance STP<br>IEEE 802.1x Port-based Network Access Control<br>IEEE 802.1ad Provider bridges – Q-in-Q stacking per VLAN/port | |

* Future implementation

# Appendix G: Release Notes for Firmware Version 2.1.6A and 3.1.4

## Introduction

Firmware Versions 2.1.6A and 3.1.4 are the new official MPLS Master-OS™ software releases for the OS900 and OS9100 models (hereafter to be collectively referred to as OS9xx). They support Layer 2, Layer 2+, and Layer 3 functionality.

## Models Supported

### Firmware Version 2.1.6A

This firmware version has 4 image files. The image file applicable to the OS9xx depends on the model, as shown in *Table 38*, below.

**Table 38: OS9xx Models and Applicable Image Files**

| No. | Model | Image File |
|---|---|---|
| 1 | OS904 (with single AC or DC power supply). | OS900-2_1_6A.ver |
| 2 | OS904-DSL4 model G.SHDSL.bis support | |
| 3 | OS904 temperture-hardened models (E and EXT) – see *Table 1*, page *58*. | |
| 4 | OS906 (with single AC or DC power supply). | |
| 5 | OS906 (with dual redundancy protected AC or DC power supply). | |
| 6 | OS912 (with dual AC or DC power supply). | |
| 7 | OS904-MBH. | |
| 8 | OS910 and the old OS912 devices (with single and dual redundancy protected AC or DC power supply). | OS900P-2_1_6A.ver |
| 9 | OS910-M – modular demarcation. | |
| 10 | OS930 – 10GE demarcation. | |
| 11 | OS9124-410G | OS9100-2_1_6A.ver |
| 12 | OS940 | OS940-2_1_6A.ver |

### Firmware Version 3.1.4

OS9xxs with firmware version 3.1.4 have ***two*** image files:

- Image file *OS900-3_1_4.ver*
- Image file *OS900P-3_1_4.ver*

The image file *OS900-3_1_4.ver* supports the following OS9xx models:

OS904 (with single AC or DC power supply)
OS906 (with single and dual AC or DC power supplies)
OS912 (with dual AC or DC power supplies)

The image file *OS900P-3_1_4.ver* supports the following OS9xx models:

OS910 and the old OS912 devices (with single and dual AC or DC power supplies).
OS910-M – modular demarcation
OS930 – 10GE demarcation

| **Note** |
|---|
| New OS912 models are designated with a “dash”, i.e., OS912-.<br>Old OS912 models are designated with a “slash”, i.e., OS912/. |

# Software Component Versions

## 2.1.6A

**OS900-2_1_6A.ver file**

Global version: 2.1.6A

Kernel version: 2.6.22.7 #595

Driver version: v1.9.3.2

Routing protocols package (ZebOS) version: 5.2

Build Time: Wed May 11 09:17:11 IST 2010

**OS900P-2_1_6A.ver file**

Global version: 2.1.6A

Kernel version: 2.6.15 #594

Driver version: v1.9.3.2

Protocols package (ZebOS) version: 5.2

Build Time: Wed May 12 09:56:41 IST 2010

**OS9100-2_1_6A.ver file**

Global version: 2.1.6A

Kernel version: 2.6.22.18 #625

Driver version: v1.9.3.2

Routing protocols package (ZebOS) version: 5.2

Build Time: Wed June 9 17:47:20 IST 2010

**OS940-2_1_6A.ver file**

Global version: 2.1.6A

Kernel version: 2.6.22.18 #625

Driver version: v1.9.3.2

Protocols package (ZebOS) version: 5.2

Build Time: Wed June 10 17:34:22 IST 2010

## 3.1.4

**OS900-3.1.4.ver file**

Global version: 3.1.4
Kernel version: 2.6.22.7 #518
Driver version: v1.4 mvPp s8624
Routing protocols package (ZebOS) version: 5.2

**OS900P-3.1.4.ver file**

Global version: 3.1.4
Kernel version: 2.6.15 #471
Driver version: v1.4 mvPp s8624

Protocols package (ZebOS) version: 5.2

# Hardware Requirements

Minimum Requirements for OS940:

CPU: FER06281, 800 MHz with 256 MB Flash and 256 MB DRAM memory.

Device hardware version of OS940: 1 or later.

Minimum Requirements for OS9100:

CPU: MV78100, 1 GHz with 128 MB Flash and 1 GB DRAM memory.

Device hardware version of OS9124: 1 or later.

Minimum Requirements for OS904, OS906, and OS912:

CPU: FER05181, 400 MHz with 32 MB Flash and 128 MB DRAM memory.

Device hardware version of OS904: 2 or later.

Device hardware version of OS904-MBH, OS906, and OS912: 1 or later.

Minimum Requirements for all other OS9xx models:

CPU: MPC8245, 266 MHz with 64 MB Flash and 256 MB DRAM memory.

Device hardware version of OS910 and the old OS912: 3 or later.

Device hardware version of OS910-M and OS930: 1 or later.

# Determining the Software version

To determine the version of the software currently running on the OS9xx, log into the OS9xx and invoke the CLI command **`show version`**.

# Upgrade Procedure

## Procedure

To upgrade/download the OS9xx image from a version that is *earlier than* 1.0.11 to version 2.1.6A or 3.1.4, the OS9xx image must first be upgraded to version 1.0.11. The image must then be run (by rebooting) and only then the version 1.0.11 may be upgraded to version 2.1.6A or 3.1.4.

Before upgrading an OS910-M having firmware version 2.1.4C or *earlier* and housing an EM9-CES-4T1C or EM9-CES-4E1C module having firmware version *CMX1624-R01.00.00_D018* to version 2.1.5 or later, first upgrade the CES module(s).

The CES module image and the document containing the procedure for downloading the image can be obtained as follows:

1. Enter MRV's knowledge base using the link http://kb.mrv.co.il/Knowledge/
2. Click on 'Carrier Ethernet Solution'
3. Click 'OptiSwitch 910-M'
4. Click on 'CES Module Firmware'

To upgrade the OS9xx with a new firmware version:

1. Log into the OS9xx.
2. Enter **`enable`** mode.
3. Invoke the command:
   **`upgrade ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME] [PASSWORD]`**
4. Wait until the completion of the upgrade process, which may last a few minutes.
5. In response to the prompt:
   `Would you like to reboot the system now ? (y|n)`
   If you want to run the new image now, type **`y`**.

If you want to run the new image at the next reboot and let the previous image keep running in the meantime, type **n**.

# Features Supported

MEF Services
EPL, E-LINE, E-TREE, and E-LAN
MEF Certification for MEF9, MEF14, and MEF21

Layer 1 Features
Virtual Cable Test (Copper TDR)
SFP Digital Diagnostics
Jumbo frames – per port/VLAN up to 16,000 bytes
Port mirroring
Port protection
Port reflection (LIN)
Port advertise capabilities for speed and duplexity

Layer 2 Bridging Features
Layer 2 transparent bridging
Layer 2 MAC learning and switching by hardware
Layer 2 Aging
Up to 16000 MAC addresses
Multiple Spanning Tree Protocol (MSTP)
G.8032/Y.1344 ITU-T Eth" Ring Protection Switching (ERPS)
BPDU Tunneling
L2 protocol tunneling of CDP, STP, VTP, PVST+, LACP, PAGP, EFM, DTP, DOT1X, ESMC, UDLD, ERPS
2 level thresholds per port for PDU storm guard
Statistics of L2 protocols such as STP, LACP, and IEEE 802.3ag
Learn table limit per VLAN/port
Link Aggregation (Etherchannel)
Link Aggregation Control Protocol (LACP)
UniDirectional Link Detection (UDLD)
Hash configuration function for Link Aggregation.
Drop Broadcast/Multicast IPv4/IPv6/Non-IP packets

Virtual LAN (VLAN) Features
4K 802.1Q-based VLANs
IEEE 802.1ad – Q-in-Q (VMAN), C-VLANs/S-VLANs
Selective VLAN forwarding, swapping/translating, stacking
Protected-ports (Private VLAN)
Hybrid Ports

Routing[107] Features -- Wirespeed
Wirespeed L3 forwarding
Routing Information Protocol (RIP I & RIP II)
Open Shortest Path First (OSPF)
Border Gateway Protocol (BGP-4)
ISIS

[107] Performed at wirespeed

Secondary addressing
Static routes
Black hole routes
Dummy Interfaces
Virtual Router Redundancy Protocol (VRRP)

Multicast
IGMP Snooping (v1, v2)
Static multicast forwarding.

Management Features
Out-of-band management
Command Line Interface (CLI) – through Serial, TELNET, or SSH (Protocol Versions 1 & 2).
Console disable
Simple Network Management Protocol (SNMP) versions 1, 2, and 3.
View-Based Access Control Model (VACM)
Remote Monitoring (RMON) - 4 groups
RADIUS authentication for management
TACACS+ authentication for management
IEEE 802.1X
Advanced management access control
Upload/Download/Append of configuration files with FTP & SCP
Copy-Paste of configuration
Time of day + Calendar + Time zone
Internal Syslog + Remote Syslog
Double tag encapsulation for management traffic
Jumbo frame support
Support MRV Provisioning and Network Management Platform
IEEE 802.3ah CO and CPE support

QoS Features
DiffServ – 8 Service levels
Trust Mode L2 / L3 / L2+L3 / Port
VPT & DSCP Marking
Traffic conditioners
Single- and Dual-Leaky-bucket policers
3 Conformance levels (green, yellow, and red)
Ingress shaping per port per queue
Egress shaping per port per queue
Accounting
Ingress and Egress Access Lists
Multiple actions in a single Access List rule
Service level accounting
Port priority
Strict Priority (SP) and Shape-Deficit Weighted Round Robin (SDWRR) Scheduling mechanisms
Hierarchical QoS up to 8 levels
Broadcast/Multicast/Unknown/TCP-syn flood limiting
Statistics per port/service-level
Logical ports to increase ingress queues

OAM – IP Service Assurance
Hardware Based IP-SLA
Extended RFC2544 frame generator support for L2 MAC frames in addition to ICMP packets

IEEE 802.1ag and ITU-Y.1731 Ethernet Service OAM
CCM packets with variable duration
Loopback – port or VLAN
Delay Measurement
Link-Trace
RDI
History of 802.1ag and ITU-Y.1731 loopback and delay-measurement
Link Protection and Link Reflection based on IEEE 802.1ag
Scheduler support for all IEEE 802.1ag and ITU-Y.1731 CLI commands
Loss Measurement support

Additional Protocols & Features
Internet Control Message Protocol (ICMP)
Internet Group Management Protocol (IGMP)
Linux Shell
Domain Name Server (DNS) Client
Network Time Protocol (NTP)
CLI/Linux shell Commands Scheduler
Cross Connect mode
Bootstrap Protocol (BOOTP)
DHCP Client
DHCP Server
DHCP Relay
DHCP Snooping

# Supported MIBs

| MIB | RFC or Private | Supports | Description |
|---|---|---|---|
| Dev-cfg.MIB | Private | NbDevRouterSaveConfig<br>Objects in the Device's Power Supplies Group (NbsDevPS) | Device General Configuration<br>Device's Power Supplies |
| Ethernet | RFC 1284 | Ethernet-like statistics group | Ethernet statistics including multicast, collision, undersize, and oversize. |
| Gswitch1 | Private | All objects (read-only) | Contains information necessary to configure/describe a port configuration. |
| Nstack | Private | Objects in the Stack Information Group (nbsStackSlotCapacity, nbsStackSlotsTableSize, nbsStackPortsCapacity, nbsStackSlotPortsCapacity)<br>Objects in the Slot Information Group (nbsStackSlotTable) | Contains information necessary for device structure including port (copper/SFP) VCT test – Copper TDR. |
| MIB-II | RFC 1213 | All objects | Contains information necessary for managing TCP/IP-based internets. |
| RMON | RFC 1757 | Ethernet Statistics, History, Alarm, Event | Contains information necessary for the RMON |

| | | | |
|---|---|---|---|
| | | | groups Ethernet Statistics, History, Alarm, Event |
| rt-cfg | Private | All objects except objects in the Device Virtual Interface Table (old) | Contains information about Device Interface Table including name and secondary interface, and limits number of interfaces of all types. |
| Switch1 | Private | All objects except nbSysSnmpCfg, nbSysTrapEntry. | Contains information about port tag outbound mode. |
| OaSwitch | Private | All objects | Contains information on Device Layer-2 Configuration and MAC Address Table of the Device |
| Tcgroup | Private | All objects | Contains information on traffic conditioner counters. It is similar to the information provided in the `tc-counters-group` mode. |
| OaSlStat | Private | All objects | Contains information about SL and status |
| DOT1AG.MIB | RFC 2863 | Read-only | Contains information on the Connectivity Fault Management module for management per IEEE 802.1ag, Draft 8. |
| nbEthOam.MIB | Private | All objects. (Private extension of the DOT1AG.MIB). | Supports groups of IEEE 802.1ag and ITU-T Y.1731. |
| osIpSla | Private | All objects | Supports groups of IP-SLA |
| osExport | Private | All objects | Supports configuration of data for export counters |
| osRfc2544 | Private | All objects | Supports the functionality of RFC2544 |
| osPort | Private | All objects | Supports the configuration & states of ports |
| Oaupgrd | Private | All objects | Supports Download/Upload software and configuration |
| osEthServ | Private | All objects | Supports the functionality of MEF Ethernet Virtual Connections |
| osServL2Cp | Private | All objects | Supports L2 Control Protocols Processing in Service Provision |
| osTdm | Private | All objects | Supports the functionality of TDM |
| IF.MIB | RFC 1573 | All objects except IfStackTable and IfRcvAddressTable | Contains information on the Interface table. |
| PING.MIB | RFC 2925 | All objects | Contains information on RTR |
| VACM.MIB | RFC 2575 | Read-only | Contains information on VACM |
| DEV-ID.MIB | Private | All objects | Contains information on the Device IDs |
| OASFP-MIB | Private | All objects | Contains information on the SFP modules |
| OADHCP.MIB | Private | All objects | Contains information on the DHCP server MIB |

| | | | |
|---|---|---|---|
| osL2PduGuard.MIB | Private | All objects | Contains information on the Layer 2 control PDU guard |
| osVif | Private | All objects | Supports functionality of tag-outbound-mode for ports |
| osProvVif | Private | All objects | Supports interfaces in the provision features. |
| osProvRfc2544 | Private | All objects | Support the functionality of rfc2544 in provision. |

# New Features Introduced in Version 2.1.6A

- This software release was tested with FPGA version **0x29** for OS904, OS906, OS912C and version **0xB** for OS9124 and OS940.
- This software release was tested with MRV Provisioning and Network Management Platform version 1.7 Beta Version.
- 802.1ag new CLI command to configure CCM alarm when the received priority bits of the ccm packet has different value than configured.
  `mep <1-4095> check-priority (error|xcon)`
- 802.1ag mep port support also trunk port.
- Provision Services Improvements:
  1. Support for configuring BW profile with CIR and CBS = 0.
  2. Multi-Flow DSCP with a non DSCP flow (to give such packets BW profile of another flow).
- **MIB changes**
  1. Oaupgrd.mib.
     - Add new enumeration downloadFpgaImageFailed (34) for the object oaDevUpgrErrorStatus.

# Features Introduced in Older Versions

Version 2.1.6

- This software release was tested with FPGA version **0x29** for OS904, OS906, OS912C and version **0xB** for OS9124 and OS940.
- This software release was tested with MRV Provisioning and Network Management Platform version 1.7 Beta Version.
- Support for the new OS940 model.
- Support for the new OS904-MBH model.
- IEEE 802.1X (Security for port Authentication) support.
  (For full details and configuration examples, refer to the OS900 Series User Manual.)
- IEEE 802.3ah support also for CO side.
  (For full details and configuration examples, refer to the OS900 Series User Manual.)
- Completion of ACL names and Action-List names by pressing the Tab key.
- G.8032/Y.1344 ITU-T Ethernet Ring Protection Switching (ERPS) improvements as follows:
  ```
  vlans VLANS_LIST
  channel-blocking
  ```
  Command `channel-blocking` configures block ports according to the VLANS_LIST configured by command `vlans`
  1. ERPS supports virtual channel/subrings (per Amendment 1).
     ```
     east-port PORT virtual-channel
     west-port PORT virtual-channel
     ```
- L2 protocol tunneling support also LAMP, DOT1X, ELMI, GARP protocol.

```
port l2protocol-tunnel
(all|cdp|pvst+|stp|vtp|dtp|pagp|udld|lacp|lamp|efm|dot1x|elm
i|lldp|garp) PORTS-GROUP [drop]
```

- Configurable 2 level thresholds per port for PDU storm guard.

```
l2-pdu-storm-guard protocol
(all|cdp|dtp|pagp|efm|dot1x|esmc|lacp|pvst+|stp|vtp|udld|ethoam
|erp) port (PORTS-GROUP|all) <0-1000> inform <0-1000>
```

  This command replaces command:

```
l2protocol-tunnel pdu-storm-guard <0-1000> PORTS-GROUP
```

- Configurable 2 level thresholds per port for PDU storm guard using SNMP system with osL2PduGuard.mib. We can also check the port state using this MIB.
- In this version All pdu storm guard thresholds **are disabled by default**.
- New CLI was added to enable 64-bit of the traffic conditioner counters (counters set 1-16) in OS900.

```
tc-counters long-counters-mode
```

- Action lists minimum rate for CIR and PIR is 0 and not 64k as in previous versions.
- Action lists minimum bucket for CBS and PBS is 0 and not 4k as in previous versions.
- Improve HQoS by adding logical ports. This will give us more queues in the ingress direction to increase the number of Customers per port.

```
port extra PORTS-GROUP
```

  (For full details and configuration examples, refer to the OS900 Series User Manual.)
- Double tag encapsulation for management traffic. When using this command all management traffic will be encapsulated with the configurable c-tag and c-vpt.

```
management c-tag <1-4095>
management c-tag <1-4095> c-vpt <0-7>
```

- ITU-Y.1731 Loss Measurement Support.
  (For full details and configuration examples, refer to the OS900 Series User Manual.)
- New CLI was added in all FPGA tests like RFC 2544, IP SLA, Y.1731 to configure the service level of the test.
  For Y.1731 tests:

```
mep <1-4095> (delay-measure|loopback) sl <1-8>
```

  For ip sla and RFC 2544 tests:

```
sl <1-8>
```

- OS9124 and OS940 Automatic Scheduler for FPGA tests to support more than 64 concurrent Tests without the need to configure a script and a scheduler.
  (For full details and configuration examples, refer to the OS900 Series User Manual.)
- 802.1ag and ITU-Y.1731 link trace is now fully supported according to the standard.
- 802.1ag CCM lowest alarm is now MAC status and not RDI as in the previous version. This is according to the standard.
- ITU-Y.1731 loopback and delay measurement can now support multiple destination MEPs and not only one as in the previous version.

```
mep <1-4095> (delay-measure|loopback|loss-measure) rmep LIST-
OF-MEPS
```

- New CLI commands to configure 802.1ag aging time of remote MEPs. The default is aging disabled.

```
remote-meps aging <0-86400>
```

- New CLI commands to configure CPU transmit queue based on packets protocols. The marking of the vpt bits is according to the global diffserv table.

```
cpu-traffic-sl transmit (ospf-rip|vrrp|isis|arp|icmp|data) <1-
8> show cpu-traffic-sl
```

- New CLI commands to configure egress counters of internal queues.
  `egress-counters (set1|set2) ingress-port (PORT|all|skip) tag (<1-4096>|all) sl (<1-8>|all) cl (green|red|all)`
- Link aggregation (trunk) are fully supported by SNMP.
- New SNMP alarms were added in osPort.mib.
  Alarm when insert or removing sfp from port (takes up to 60 second to be sent).
  Alarm when disable or enable a port.
- New CLI commands for IGMP were added:
  1. Send all IGMP protocol packets with SOURCE-IP=0.0.0.0. If IP subnet is not defined on the interface.
     `zero-source-ip`
  2. Display IGMP ports.
     `show igmp-port PORTS-GROUP`
  3. Display IGMP protocol packets statistics.
     `show igmp-statistics PORTS-LIST`
  4. Clear IGMP protocol packets statistics.
     `clear igmp-statistics`
  5. Display all multicast-IP entries per client port.
     `show mc-ip port PORTS-LIST`
  6. Display Multicast forwarding entries for one specific TAG only.
     `show mc-ip vid TAG`
  7. Enable IGMP proxy.
     `mode igmp-proxy`
  8. Enable Purely passive forwarding of Mcast group and flooding of IGMP packets.
     `mode pure-snooping`
  9. Enable QUERY flooding and non-QUERY IGMP packets proxy.
     `mode query-flooding`
  10. Disable Purely passive forwarding of Mcast group and flooding of IGMP packets and enable IGMP proxy (default mode).
      `no mode pure-snooping`
  11. Disable QUERY flooding and non-QUERY IGMP packets proxy and enable IGMP proxy (default mode).
      `no mode query-flooding`
  12. Enable special mode: Don't send Query Specific packet in Leave process.
      `no query-specific`
  13. Disable special mode "Don't send Query Specific packet in Leave process", and return to default mode: Send Query Specific packet in Leave process (default).
      `query-specific default`
  14. To define IP address that is used in the IGMP-query (general & specific) packets as Source IP address in IP header.
      `query-specific-ip A.B.C.D`
  15. Don't use special IP address as Source IP address in IP header of the IGMP-query Packets.
      `no query-specific-ip`
- New CLI commands to improve interface statistics on OS9124 only:
  1. Vlan statistics are divided between ingress which is always enabled And egress which is disabled by default.
     To enable egress statistics:
     `vlan-egress-counters`
  2. Show statistics on all interfaces.
     `show interface-vlan-counters`
     `monitor interface-vlan-counters`
  3. Show statistics on specific interfaces.

```
show interface-vlan-counters TAG lines  LINES
monitor interface-vlan-counters TAG lines  LINES
OS9124# show interface statistics
```

4. Clear vlan statistics.

```
clear interface-vlan-counters
OS9124(config-vif2)# clear interface-vlan-counters
```

- New CLI commands to improve port egress statistics on OS9124 and OS940:

Port egress counters are enabled by default.

```
show port egress-counters (byte|packet|all) [PORTS_GROUP]
show port egress-counters (byte|packet|all) details [PORTS_GROUP]
monitor port egress-counters (byte|packet|all) [PORTS_GROUP]
monitor port egress-counters (byte|packet|all) details [PORTS_GROUP]
```

- When radius server is configured and the login was made from the local we get different prompt
- New CLI commands under boot node.
  1. Enable SSH version 2 only.
     `sshd-protocol-version 2`
  2. Enable sftp server.
     `sftp-server enable`
  3. Enable view node show commands. (this will add more show commands to the view node).
     `view-commands enable`
- Provision Services improvements:
  1. Support for OS9124 and OS940.
  2. RFC 2544 support include new mibs osProvRfc2544.mib and osProvVif.mib.
  3. Support for port mtu was added.
  4. Support for multiple destination MEPs.
  5. Aging time of remote MEPs support and CCM clean support.
  6. C-vlan preservation support.
  7. Aggregation Services support.
- MIB changes

1. nbEthOam.MIB
   – Last history index was added to loopback and delay measure tables.
   – Support for multiple destinations for loopback and delay measure tables.
   – LastPriority value was changed from read-write to read-only.
   – New objects in Alarms parameters: HistDestMepId, HistDestMepMac,LastHistIndx.
2. Dev-cfg.MIB.
   – Extension for temperature info
3. nstack.MIB
   – Support XFP copper
4. osPort.MIB
   – New alarms were added
   – New L2 protocols: DTP, PAGP
   – Added ERPS for block reasons
   – Port trunk support in IfType
5. osRfc2544.MIB
   – Last history index was added to the results table
   – Default value for MinStep was fixed for 1000
   – Default value for ProbeInterval was fixed for 100000
6. Oaupgrd.MIB

   - Added new Objects of LocalFile and removeLocalFile to support upgrade from the Device
7. UCD-SNMP-MIB.MIB
   - Support of CPU utilization. New Mib was taken from UCD-SNMP
8. osEthServ.MIB
   - Lowest Alarm is MAC status and not RDI
   - Changing ingress C-VLAN support
   - CCM clean and remote MEP aging time support
   - Aggregation support
   - Lock and Unlock for Admin status
   - Support for multiple destinations MEPs
   - Deletion of the following objects:
     osEthServMepId, osEthServPerfPrfl, osEthServPerfEnabled, osEthServPerfDestMacAddress, osEthServPerfDestMepId, osEthServPerfDestIsMepId, osEthServIngBwPrfl, osEthServIngBwAccStatus, osEthServEgBwPrfl, osEthServEgBwAccStatus, osEthServFlowMepDirection, osEthServFlowPerfDestMepList.

Version 2.1.5D

- This software release was tested with FPGA version 0x29.
- 802.1ag remote MEPs aging is now disabled by default.
- Link reflection for OC3 modules.
  **`link-reflection-ces uplink PORT downlink (p1|p2) (direct|inverse) symmetrical`**
- DSL improvements:
  1. Enlarged PAF timeout from 20 to 255 seconds (like in standard).
  2. Improved LED blinking.
  3. Fixed sign issue at actual SNR values to show negative values properly.

Version 2.1.5C

- This software release was tested with FPGA version 0x29.
- New CLI command to show Tech-Support information.
  **`show tech-support`**
- L2 protocol tunneling support also UDLD, PAGP, DTP protocol.
  **`port l2protocol-tunnel (all|cdp|pvst+|stp|vtp|dtp|pagp|udld|lacp) PORTS-GROUP [drop]`**
- Hot Swap for TDM modules.
  **`tdm module remove slot (2|3)`**
  **`tdm module insert slot (2|3)`**
- When port is down clear the learning table entries of this port.
  To enable this mode use the CLI command:
  **`lt clear-port-link-down`**
- In CLI command "time" we added the option to configure also the seconds.
  **`time TIME`**
- CLI command "show link-reflection" also return the port state.

Version 2.1.5

- This software release was tested with FPGA version 0x29.
- Support for OS900 equipped with FPGA to run 64 concurrent tests with frame generator at up to 1Gbps full wirespeed.
- Support for the new OS904-DSL4 model G.SHDSL.bis.
- This version fully supports the MRV ProVision Provisioning and Network Management Platform.

- G.8032 / Y.1344 ITU-T Ethernet Ring Protection Switching (ERPS).
  For details and configuration examples refer to the OS9xx User Manual.
- RFC 2544 frame generator extended support for Layer 2 frames in addition to ICMP frames.
  For details and configuration examples refer to the OS9xx User Manual.
- RFC 2544 new mib file to configure and show results using SNMP osRfc2544.mib
- RFC 2544 performance thresholds were added.
  **threshold (frame-delay|jitter) rise <0-100000> fall <0-100000>**
  **threshold packet-loss rise <0-100> fall <0-100>**
- Automatic Scheduler for FPGA tests to support more than 4 concurrent tests without the need to configure a script and a scheduler.
  Supported tests: IP SLA, Loopback, and Delay Measurement.
  For details and configuration examples refer to the OS9xx User Manual.
- OAM pdu-storm-guard is disabled by default in this version.
- Upgrade version of FPGA using SNMP system with Oaupgrd.mib.
- Batch upgrade using SNMP system with Oaupgrd.mib.
- Show version of FPGA using SNMP system with dev-id.mib.
- New CLI mode to easily configure new services using high level CLI commands.
  For details and configuration examples refer to the OS9xx User Manual.
- New CLI command to configure port layer2 loopback. This commands swaps the destination MAC address with the source MAC address
  **port layer2-loopback PORT_INDEX**
- New extended ACL classification for untagged frames.
  **tag eq any**
  **tag eq untagged**
- TACACS+ ASCII authentication method was added.
  **tacacs-server host (A.B.C.D|HOSTNAME) authen-method (ascii-login|pap-ppp)**
  **tacacs-server authen-method (ascii-login|pap-ppp)**
- Several accounting levels for TACACS+ (login,enable,Configure,debug)
  **accounting commands (login|enable|configure|debug) (radius|tacacs+)**
- Suppport new CES OC-3/STM-1 module and EVC per E1 session for OS910-M and OS9124-410G.
  For details and configuration examples refer to the OS9xx User Manual.
- TDM Module alarms /traps were Added using osTdm.mib.
  TDM Module Generic Alarm.
  TDM Module Port Alarm.
  TDM Module Clock Alarm.
  TDM Module Session Alarm.
  TDM Module Interface Alarm.
- DHCP/Bootp client per interface.
  **ip dhcp**
  **ip dhcp client broadcast**
  **ip dhcp client timeout TIMEOUT**
  **ip dhcp client timeout unlimited**
- Show port details also returns the Up/Down time (availability) of each physical port.
- New CLI command to copy tech-Support params into file and upload it using ftp or scp.
  **copy tech-support (ftp|scp) SERVER REMOTE-DIR [USERNAME] [PASSWORD]**
- New CLI command to change MTU to be forwarded to CPU port.

`mtu MTU`

Note: This command may effect routing protocols.

- L2 protocol tunneling per MAC address can now be configured.
  `l2protocol-tunnel mac MAC_ADDRESS`
- L2 protocol tunneling support also LACP protocol.
  `port l2protocol-tunnel (all|cdp|pvst+|stp|vtp|lacp) PORTS-GROUP [drop]`
- New CLI command to configure l2protocol-tunnel PDU storm guard (default: 50 pps).
  `l2protocol-tunnel pdu-storm-guard <0-1000> PORTS-GROUP`
- New port redirect action for Software based ACL for l2-protocols.
  `action redirect ports PORTS-GROUP`
- DHCP snooping + option 82 for 3 fields : hostname, source port,VLAN support.
  For details and configuration examples refer to the OS9xx User Manual.
- New CLI command to ignore a list of remote MEPs.
  `[no] ignore-rmeps (all|LIST-OF-MEPS)`
- New CLI command to disable OAM CCM alarms.
  `[no] ethernet oam trace-ccm-fault`
  `[no] mep <1-4095> trace-ccm-faults`
- CLI command `show buffers under-use` also returns buffer usage of internal queues.
- New CLI command to display configured link reflection data `show link-reflection`.
- New CLI command:
  `link-protection primary PORT1 rmep DOMAIN1 SERVICE1 RMEP1 backup PORT2 rmep DOMAIN2 SERVICE2 RMEP2`
- New Rapid Ping to support rate, size, ToS.

```
ping WORD [COUNT]
ping WORD count COUNT rate (RATE|rapid)
ping WORD count COUNT rate (RATE|rapid) size SIZE
ping WORD count COUNT rate (RATE|rapid) size SIZE source SOURCE
ping WORD count COUNT rate (RATE|rapid) size SIZE source SOURCE tos <0-254>
ping WORD count COUNT rate (RATE|rapid) source SOURCE
ping WORD count COUNT size SIZE
ping WORD count COUNT size SIZE source SOURCE
ping WORD count COUNT source SOURCE
ping WORD rate (RATE|rapid)
ping WORD rate (RATE|rapid) size SIZE
ping WORD rate (RATE|rapid) size SIZE source SOURCE
ping WORD rate (RATE|rapid) source SOURCE
ping WORD size SIZE
ping WORD size SIZE source SOURCE
ping WORD source SOURCE
```

- New EXPORT DATA node, used to configure parameters for collect and transfer different counters also can be configured by SNMP using osExport.mib.
  `export NAME`
  Configure client ID
  `client id ID`
  Configure / delete export entry description
  `[no] description ...`
  Configure remote server for transfer data

`server address (A.B.C.D | HOSTNAME)`

Configure / delete remote directory

`remote dirname NAME`

`no remote dirname`

Configure / delete remote filename

`remote filename NAME`

`no remote filename`

Configure / delete remote user name

`remote username NAME`

`no remote username NAME`

Configure / delete remote user password

`remote password PASSWORD`

`no remote password`

Configure transfer data block size (in samples)

`transfer block-size <1-2000>`

Configure transfer data protocol

`transfer protocol (ftp | scp)`

Configure sample frequency – data collection interval

`sample frequency (once | monthly | weekly | daily | 12hrs | 8hrs | 6hrs | 4hrs | 2hrs | 1hr | 30mins | 15mins | 10mins | 5mins | 2mins | 1min)`

Configure start data collection time

`start time TIME`

Enable / disable export data entry

`enable`

`no enable`

Version 2.1.4C

- Number of IP subnets increased from 10 per interface (in previous versions) to 15.
- IP address of an interface can now be removed on the fly., i.e., there is no need to disable the interface before removing the IP address.
- The following BOOTP options were added.
  1. Management. The BOOTP interface can now be managed.
     `bootp-option management`
  2. Configure the TFTP timeout, i.e., Max-Time to wait for configuration via TFTP.
     `bootp-option tftp-timeout TIMEOUT`
  3. Configure the retry interval.
     `bootp-option retry-interval RETRY_INTERVAL`
- New CLI command to stop the dhcp-client was added.
  `bootp stop` ( this command is hidden).
- TACACS+ ASCII authentication method was added.
  `tacacs-server host (A.B.C.D|HOSTNAME) authen-method (ascii-login|pap-ppp)`
  `tacacs-server authen-method (ascii-login|pap-ppp)`
- New CLI command to clear all ARP entries was added.
  `no arp (all|HOSTNAME) [IFNAME]`

Version 2.1.4B

- Before upgrading, make sure you have the 12-digit ***activation key*** for installation. If not, please contact MPLS@mrv.com to receive it.
- This software includes all features and bug fixes of ***version 2.1.4B***.
- The OSPF code was optimized for better performance.

- OSPF RFC 4222 (see http://tools.ietf.org/html/rfc4222) was implemented.
  See application notes document (filename *OSPF_application_note.doc*).

**OSPF RFC 4222 CLI Commands**

`prioritized-treatment inactivity-timer`

Hold-time is reset for every incoming unicast packet per RFC 4222 recommendation 1.

`debug ospf prioritized-treatment inactivity-timer`

Activate printing of debug information (related to this feature) to the syslog.

`prioritized-treatment retransmit-interval <1-7> <3-65535>`

Use an exponential back-off algorithm for determining the value of the retransmission interval for LSAs. The first input value defines the **K** parameter of the algorithm and the second value defines the maximum interval in seconds.

`debug ospf prioritized-treatment retransmit-interval`

Activate printing of debug information (related to this feature) to the syslog.

`prioritized-treatment lsa-pacing boundaries HIGH LOW gap-factor <1-5> consistency <1-5>`

Configure the rate at which LSAs are sent to a neighbor that is suspected of being congested. This rate follows an exponential back-off algorithm explained in detail in the application note.

`debug ospf prioritized-treatment lsa-pacing`

Activate printing of debug information (related to this feature) to the syslog.

`prioritized-treatment throttling-adjacencies max-num <1-5> retry-interval <1-0>`

`prioritized-treatment throttling-adjacencies max-num <1-5> retry-interval <1-20>`

`prioritized-treatment throttling-adjacencies max-num <1-5>`

OSPF adjacencies are formed gradually, i.e., no more than the configured maximum amount of adjacencies are formed concurrently. The user can set the interval during which the OS900 is to retry to establish new adjacencies.

`debug ospf prioritized-treatment throttling-adjacencies`

Activate printing of debug information (related to this feature) to the syslog.

`timers pacing flood <5-300>`

Set the transmission rate of LSAs (unicast and broadcast) strictly according to the set millisecond value of the argument.

`show ip ospf refresh-list`

Show the different LSA groups created in the refresh-list database to enable the user to create changes in the “refresh-list timers” setting and to pace the LSAs accordingly during the refresh time period.

- ISIS code was optimized for better performance.

**ISIS CLI Commands**

`passive-interface IFNAME [ A.B.C.D]`

Suppress IS-IS packets received/transmitted on the given interface (and IP)

`passive-interface default`

Suppress IS-IS packets received/transmitted on the all interface

`no passive-interface default`

Restore the ability of all interfaces to received/transmitted IS-IS packets.

`redistribute {bgp|connected|kernel|ospf|rip|static} route-map RMAP_NAME`

`redistribute (kernel|connected|static|rip|ospf|bgp) metric <0-4261412864> route-map WORD`

`redistribute (kernel|connected|static|rip|ospf|bgp) (level-1|level-1-`

```
2|level-2) metric <0-4261412864> metric-type (internal|external)
route-map WORD
redistribute (kernel|connected|static|rip|ospf|bgp) (level-1|level-1-
2|level-2) metric-type
(internal|external) metric <0-4261412864> route-map WORD
redistribute (kernel|connected|static|rip|ospf|bgp) metric <0-
4261412864> (level-1|level-1-
2|level-2) metric-type (internal|external) route-map WORD
redistribute (kernel|connected|static|rip|ospf|bgp) metric <0-
4261412864> metric-type
(internal|external) (level-1|level-1-2|level-2) route-map WORD
redistribute (kernel|connected|static|rip|ospf|bgp) metric <0-
4261412864> route-map WORD
redistribute (kernel|connected|static|rip|ospf|bgp) metric-type
(internal|external) (level-1|level-
1-2|level-2) metric <0-4261412864> route-map WORD
redistribute (kernel|connected|static|rip|ospf|bgp) metric-type
(internal|external) metric <0-
4261412864> (level-1|level-1-2|level-2) route-map WORD
```

Adding route-map classification mechanisms to all IS-IS redistribution capabilities

- LDP CLI commands.

```
mpls l2-circuit VC_NAME regards-ac-state
```

Regarding the AC (Attachment Circuit) state in the MPLS status: By default, it is no longer needed to have the MPLS access port in a "link up" state in order to have the VC operational.

The above command will make it mandatory to have the VC AC in an UP state for the entire VC to be up.

```
targeted-peer DEST_IP pw-status-disable
```

PW status implementation according to RFC 4447: In previous versions every change in the PW state triggered sending of “label withdrawn" packet. Following the implementation of RFC 4447 additional information can be supplied to describe the VC state using the PW-Status packets. The new default behavior of the machine is to send PW-Status packets instead of Label-withdraw. The above command disable the new mechanism and the original label-withdraw option is used.

```
mpls l2-circuit virtual-port-reflection
```

This proprietary MRV feature works like the L2 port reflection, only on the two sides of the MPLS cloud. When the access port on one side goes down the same will happen to the access port on the remote side. This proprietary MRV feature solves deadlock scenarios in the spanning tree topology.

By default, this feature is not activated.

- Add Routing/MPLS protocols performance tool.
  See application-notes document (file name OSPF_application_note.doc).

```
show thread cpu (nsm | isis | bgp | rip | ospf | ldp | rsvp)
```

Presents statistical information on the given protocol pseudo-threads (ave. time of run, maximum time of run, number of time the thread was called etc.)

```
clear thread cpu (ldp|rsvp|isis|nsm|bgp|rip)
```

clears the statistical information gathered for the specific protocols.

- osIpSla.mib was changed. All measurement values in the MIB are now in microseconds for both cpu and hardware tests.

Version 2.1.4A

- Add new CLI command for upgrading with no reboot after the upgrade is successfully finished.

```
upgrade no-reboot ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME
[USERNAME] [PASSWORD]
upgrade no-reboot scp SERVER REMOTE-DIR REMOTE-FILENAME USERNAME
PASSWORD
```

- Automatic detect on startup for SFP100-FX. After booting the OS900 will check if an SFP100-FX was inserted and if so it will automatically set the **`port media-select`** parameter to the value **`sfp100`**.
- Software based ACL for l2-protocols improvements: Classification of tag field is optional. If no tag was configured the rule applies for all tags.
- Note: Recommended FPGA version is **`0x25`**.

Version 2.1.4

- CLI command `port state (enable|disable) (PORTS-GROUP|all)` support also members in Trunk group.
- Add new CLI command to configure LACP timeout timers (default is 3 seconds)

```
lacp timers timeout <3-60>
```

- Add new CLI command to disable fiber port bypass mode.(bypass is enabled by default).

```
no port bypass (PORTS-GROUP|all)
```

- Add new CLI command to configure copper port cross-over mode

```
port crossover-mode (mdi|mdix|auto) (PORTS-GROUP|all)
```

- Add new CLI command for upgrading with automatic reboot after the upgrade is successfully finished.

```
upgrade force-reboot ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME
[USERNAME] [PASSWORD]
upgrade force-reboot scp SERVER REMOTE-DIR REMOTE-FILENAME
USERNAME PASSWORD
```

- Periodic egress counters.The counter automaticly count each port individualy for 1 minute and in case of packet drops on a specific port a message is sent to the syslog file.

```
egress-counters (set1|set2) port (PORT|all|skip) tag (<1-
4096>|all) sl (<1-8>|all) cl (green|red|all)
```

- Software based ACL for l2-protocols. In this version we have 50 ACL rules. Each rule has classification fields of protocol, tag and src-phy-port and action fields for tag nest and mark vpt. The commands are identical to the extended ACL.

```
l2protocol-tunnel rule <1-50>
```

  For full details and configuration examples read the OS900 User Manual.
- Show buffer usage of each port on every queue.

```
show buffers under-use [PORTS-GROUP]
```

- Add new CLI command to configure packet-loss Performance Monitoring (Y.1731) threshold.
  This command is in ethernet oam service node.

```
mep <1-4095> threshold packet-loss rise <0-100> fall <0-100>
```

- CLI command of 802.1ag c-ports PORTS-GROUP is now per service or per domain.
  (In previous version it was per domain only).
- Add support for dot1agCfmMepDbTable in dot1ag.mib.
- Performance Measurement (Y.1731): Priority field and packet loss were added to the history and test type was also added to specify if the test was running from hardware or from CPU.
  To support it also for SNMP we Add the following objects in nbEthOam.mib:

```
nbEthOamLbHistType, nbEthOamLbHistPriority,
nbEthOamLbHistPcktLoss
```

- IP-SLA: L3 Performance Measurement: Priority fields were added to the history and also error reports for wrong sequence, time out, rx errors, tx errors were added.
  To support it also for SNMP we Add the following objects in osIpSla.mib:
  ```
  osIpSlaResultsTimedOut , osIpSlaResultsWrongSequenced ,
  osIpSlaResultsRxErrors, osIpSlaResultsSendFailed ,
  osIpSlaResultsHistoryRows , osIpSlaResultsPriority,
  osIpSlaResultsTos
  ```
- RFC 2544: Network Performance Testing: loss ratio and steps were added for the automatic Throughput test.
  loss ratio means the percentage of traffic you allow to loose and still pass the test.
  ```
  step STEP
  loss-ratio <0-100>
  ```
- Extended ACL: TCP flags classification was added.
  ```
  tcp-flags eq HEX_VALUE [MASK_HEX_VALUE]
  ```
- Periodic egress counters.The counter automaticly count each port individualy for 1 minute and In case of drops on a specific port a message is sent to the log file.
  ```
  egress-counters (set1|set2) port (PORT|all|skip) tag (<1-
  4096>|all) sl (<1-8>|all) cl (green|red|all)
  ```
- Show buffer usage of each port on every queue.
  ```
  show buffers under-use [PORTS-GROUP]
  ```
- Extended ACL: a new action was added for matching counters.
  There are 32 matching counters that count how many packets went through this rule.
  ```
  action matching-counter-set <1-32>
  monitor access-list extended-matching-counter <1-32>
  show access-list extended-matching-counter <1-32>
  clear access-list extended-matching-counter <1-32>
  ```
- Add new CLI command to copy the startup configuration to a specific file on remote server using ftp or scp.
  ```
  copy startup-config ftp FTP-SERVER REMOTE-DIR remote-file
  FILENAME [USERNAME] [PASSWORD]
  copy startup-config scp SERVER REMOTE-DIR USERNAME  PASSWORD
  [FILENAME]
  ```
- Add new CLI command to configure tacacs+ authorization. The authorization has Four node options: login, enable , debug, configure.
  ```
  authorization (login|enable|debug|configure) tacacs+
  ```
- Add new CLI command to configure tacacs+ encript key (sha2 encryption).
  ```
  tacacs-server encrypt key
  ```
  This CLI command will encrypt the key which was configured using the CLI command:
  ```
  tacacs-server key LINE
  ```
- Tacacs Keys are now up to 100 characters. (The key doesn't support spaces and tabs).
- Add new CLI command for upgrading with automatic reboot after the upgrade is successfully finished.
  ```
  upgrade force-reboot ftp FTP-SERVER REMOTE-DIR REMOTE-FILENAME
  [USERNAME] [PASSWORD]
  upgrade force-reboot scp SERVER REMOTE-DIR REMOTE-FILENAME
  USERNAME PASSWORD
  ```
- Software Optimizations: All the show commands were removed from configure node.
- Add new CLI command to configure performance level. The default is level 1.
  This command is very useful when doing automatic testing with testers like SmartBit, Ixia.
  ```
  performance-level (level-1|level-2|level-3|level-4|level-5)
  ```

- Add new CLI command to configure the number of dying gasp traps we are sending in case of power failure.
  ```
  efm-cpe dying-gasp-trap <1-30>
  show efm-cpe dying-gasp-trap
  ```
  In case of a recovery after a power failure a recover trap is also send.
- Add new CLI command show EFM capabilities.
  ```
  show efm-cpe cfg-capability
  ```
- Note: Recommended FPGA version is **0x25**.

Version 3.1.2

- MPLS features
  - Label Distribution Protocol (LDP)
  - Constrained Routing Label Distribution Protocol (CR-LDP)
  - Resource Reservation Protocol with Traffic Engineering (RSVP-TE)
  - Virtual Private Networks (VPNs) – Martini draft
  - Hierarchical Virtual Private LAN Service (H-VPLS)
  - E-LSP
  - H-VPLS Dual Homing
  - MAC withdraw as per H-VPLS specifications
- Supported RFC’s:
  - RFC 3031 MPLS Architecture
  - RFC 3032 MPLS Label Stack Encoding
  - RFC 3036 LDP specifications
  - RFC 3037 LDP Applicability
  - RFC 3063 MPLS loop prevention mechanism
  - RFC 3209 Extentions to RSVP for LSP
  - RFC 3210 Applicability statement for extentions to RSVP for LSP tunnels
  - RFC 3212 CR-LDP
  - RFC 4762 VPLS Using Label Distribution Protocol (LDP) Signaling
- Supported IETF Drafts:
  - draft-IETF-L2circuit-trans-MPLS-08
  - draft-IETF-L2circuit-encap-MPLS-04
  - draft-IETF-PWE3
  - draft-IETF-ppvpn-vpls-ldp (H-VPLS spoke PE-r)
  - draft-IETF-MPLS-lsp-ping-09
- Added new CLI command for SNMP link trap parameters
  ```
  link-trap-parameters (all|cisco|ietf|legacy)
  ```

**For full details and configuration examples refer to the OS900 Series User Manual.**

Version 2.1.3

- IP-SLA: L3 Performance Measurement (Y.1731) extension at Nanosecond accuracy for IP-VPN networks.
  A new mib file was added to support ip sla configuration and test results reading using SNMP. Mib file name is osIpSla.mib.
  For full details and configuration examples read the OS900 User Manual.
  **NOTES:** **1.** To support this feature an upgrade to **FPGA version: 0x1F** is required.
  **2.** This feature **replaces the RTR** feature from older versions. If you are using the RTR **do not upgrade** to this version.
- RFC 2544: Network Performance Testing.
  - Automatic Throughput testing to calculate the rate with zero frame loss.

- Packet size up to 9K Bytes.
- Jitter and Latency with nano second accuracy.
- CoS marking of IP ToS and L2 VPT (802.1p) fields.

For full details and configuration examples read the OS900 User Manual.

**NOTES: 1.** To support this feature an upgrade to **FPGA version: 0x1F** is required.

**2.** In the current FPGA version 0x1F the **maximum** recommended rate for this release is 750Mbps. Rate above 750Mbps may incounter inaccurate results.

- When Using Performance Measurement (Y.1731) extension with this version an upgrade to **FPGA version: 0x1F** is required.
- Added nbEthOamCapabilities object to nbEthOam.mib file to support tests from hardware
  and from CPU.
- Support RFC 3021 for /31 mask bit of ip address.
- Add new CLI command to configure customer ports for 802.1ag. On those ports for this domain we will not transmit CCM packets.
  This command is in the domain node.
  ```
  c-ports PORTS-GROUP
  ```
- Add new bootp options.
  ```
  bootp-option preload-config
  bootp-option vendor-class-identifier VENDOR_ID
  ```
- Add new CLI command for SNMP link trap parameters for compatibility with 3rd party NMS/OSS – Add more details
  ```
  link-trap-parameters (all|cisco|ietf|legacy)
  ```
- Add new CLI command for upgrade the firmware using scp protocol.
  ```
  upgrade scp SERVER REMOTE-DIR REMOTE-FILENAME USERNAME PASSWORD
  ```
- Bridge interface was added.The Bridge is between the in-band Interface and the out-of-band Interface (eth0).
  For full details and configuration examples read the OS900 User Manual.
- Add service password encryption for ISIS and BGP protocols.
- ACL rules which are not active will return status disable and not invalid as previous versions.
- Add new CLI command in scheduler extended to disable the executed command log messages.
  ```
  no log commands
  ```

Version 2.1.2

- Support for the new OS906 (with single and dual power supplies).
- Support for the new LD OPN1600-8C2 switch module.
- Link OAM 802.3ah passive mode for OS900.
  Support for autodiscovery, Dying Gasp & SNMP trap, and remote loopback. The loopback swaps the source MAC address with the destination MAC address.
  For full details and configuration examples refer to the OS900 User Manual.
- Analyzer VLAN for the new OS912 can now be configured using:
  ```
  OS912C(config-boot)# analyzer-vlan
  ```
  This CLI command is in the boot mode so that reboot must be done for it to take effect.
  **Note**: If analyzer VLAN is configured on Port 10 of the OS912 the *internal* port 10 will cease to exist after reboot, so that “extra ACL” and “ingress shaping” cannot be applied to this port.
- Performance Measurement (Y.1731) extension with microsecond accuracy.
  **Note**: To support this feature, upgrade to **FPGA version 0x19** is required.
  For full details and configuration examples refer to the OS900 User Manual.
- Generation of synthetic (internally-produced) traffic of rates of up to 1 GigE based on Y.1731 Performance Management
  **Note**: To support this feature, upgrade to **FPGA version 0x19** is required.

- Extended private MIB Y.1731 was enhanced and now also contains the last measurement result and a new SNMP trap for CCM fault/clear and a new SNMP trap for threshold of Jitters and Delay Measurements.
- A new CLI command was added to show the 802.1ag CCM packets interval:
  `show ccm interval`
- A new CLI command was added to show default values of the 802.1ag and Y.1731:
  `show ethernet oam defaults`
- Classification of EXP bits of an MPLS label:
  `mpls-exp-tagged eq <0-7>`
  `mpls-exp-untagged eq <0-7>`
  New profile:

  To classify EXP bits, a new ACL mpls-exp profile must be configured:

  `access-list extended-profile (normal|double-tag|mpls-exp)`

  Legality:

  - Change available profile when all the ACLs are unbound.
  - The binding process fails when the rule does not match its profile ('mpls-exp-tagged' with normal or double-tag profile).
  - ACL with 'mpls-exp-tagged' or 'mpls-exp-untagged' cannot be bound to an egress port.
  - Classification of 'mpls-exp-tagged' or 'mpls-exp-untagged' fields cannot be combined with L3 and L4 classification fields in the same rule.
- New action was added to ACL: 'redirect to cpu port'. Use this action if a rate limit is needed for traffic going to the cpu. Otherwise use 'trap-to-cpu' action.
  `action redirect port cpu`
- Filtering rules for control protocols (CDP, VTP, PVST, BPDU) do not impact ACLs or STP operation for BPDU blocking
  `port l2protocol-tunnel (all|cdp|pvst+|stp|vtp) PORTS-GROUP [drop]`
- Save mode for multiple configuration files (up to 5 files).
  For saving a new configuration file use:
  `write file NAME`
  For a list of all configuration files use:
  `show file`
  For showing which file is in use use:
  `show boot-config-file`
  For deleting a configuration file use:
  `delete conf NAME`
  For switching between configuration files use:
  `boot-config-file FILE`
  A reboot is needed for the new file to be loaded.
- Link flap guard is now per port and not global.
  The default state for this feature is disabled.
  `link-flap guard <5-10000> port (PORTS-GROUP|all)`
- Extended statistics per port on a trunk
  When the CLI command `show port statistics` is applied to a trunk port, statistics for each member of the trunk can be viewed.
- Show version number of the backup partition (image)
  `show version backup`

- BootP extensions (broadcast, timeout , ETH0, and Bridge interfaces option)

```
bootp eth0
bootp eth0 bridge BRNAME
bootp-option broadcast-always
bootp-option timeout TIMEOUT
bootp-option timeout unlimited
```

- CLI command to configure port's MTU size can also be applied to trunk ports.

```
port mtu-size (PORTS-GROUP|all) <64-16000>
```

- NTP time zone simplification
  For full details and configuration examples refer to the OS900 User Manual.

Version 2.1.1

- Support for the new OS912 with 64MB flash and 256MB DRAM memory.The new OS912 also has an FPGA to support new features in hardware.
  **Note**: Ports 11 and 12 of the new OS912 do not have internal ports (Just like the old OS912) so “extra ACL” and “ingress shaping” can’t be applied to those ports.
- Support for upgrade of the FPGA code to support new features in hardware (Only on OS912 and OS904).

Steps for upgrading:

1. Copy the FPGA file from an ftp server:
   ```
   copy ftp fpga FTP-SERVER REMOTE-DIR REMOTE-FILENAME [USERNAME]
   [PASSWORD]
   ```
2. Copy the file to the FPGA:
   ```
   upgrade fpga
   ```
3. Show the FPGA version:
   ```
   show fpga version
   ```
4. Remove local copy of file:
   ```
   remove fpga-file
   ```

- Multicast Features
- IGMP Snooping(v1, v2).
- Static multicast forwarding.
  For full details and configuration examples read the OS900 User Manual.
- UniDirectional Link Detection (UDLD) protocol

```
port udld aggressive [PORTS-GROUP]
port udld enable [PORTS-GROUP]
port udld message-interval  <7-90> [PORTS-GROUP]
port udld primary-vlan <1-4095> [PORTS-GROUP]
port udld reset [PORTS-GROUP]
port udld slow-message-interval  <7-90> [PORTS-GROUP]
```

- Port Advertise. Advertise default auto-negotiation capabilities

```
port advertise speed (10|100|1000|all) duplex (half|full|all)
(PORTS-GROUP|all)
```

- Link flap guard
  Isolate port changing link state with very high frequency (default 10 changes per second). The CLI command configures link flap guard limit:

```
link-flap guard <5-500>
```

CLI commands restore default link flap guard limit:

```
link-flap guard default
no link-flap guard
```

- Port link flap dampening
  Ability to isolate port changes its link status with the high frequency.
  The CLI command enables link flap dampening for selected ports:

  **port errdisable detect cause link-flap PORTS-GROUP**

  The CLI command recovers ports are isolated by link flap dampening mehanism:

  **port errdisable recover cause link-flap PORTS-GROUP**

  The following CLI commands configure link flap dampening:
  **link-flap-dampening errdisable-threshold VALUE**
  **link-flap-dampening recovery-threshold VALUE**
  **link-flap-dampening flap-penalty VALUE**
  **link-flap-dampening stability-grant VALUE**
  The CLI command display port link flap dampening state:
  **show port link-flap-dampening PORTS-GROUP**

- New CLI commands to display list of tags defined on the port.
  **show port tag PORTS-GROUP**

  **show port details PORTS-GROUP**

- Link protection status : show port details gives us information about who is active.

```
OS904(config)# show port details t1
Trunk t1 details:
-------------------
Description                : N/A
Link                           : OFF
Duplex state               : N/A
Speed selected             : AUTO
Auto-Neg Advertise  : Default
State                           : ENABLE
Priority                       : 1
Flow control mode     : off
Ethertype                    : CORE1:0x8100
OutBound Tagged      : untagged
Tags List                    :
Udld                           : -
Link-protection            : primary 3 and backup 4 with preemption. Now active is 4.
```

- Link protection SNMP traps. The device sends SNMP traps when we switch ports in link protection. The trap also include information of which port is active.
- Port qos trust mode now support trunk ports

**port qos-trust (PORTS-GROUP|all) (port|l2|l3|l2l3)**

- Port qos marking mode now support trunk ports

**port qos-marking (PORTS-GROUP|all) (vpt|dscp|vptdscp)**

- Port ingress and egress shaping now support trunk ports.
  The rate applies to <u>each member of the trunk and is not the total rate of the entire trunk</u>.

  **port egress-shaping per-queue <1-8> rate RATELIMIT burst-size BURSTSIZE (PORTS_GROUP|all)**

  **port egress-shaping rate RATELIMIT burst-size BURSTSIZE (PORTS_GROUP|all)**

  **port ingress-shaping per-queue <1-8> rate RATELIMIT burst-size BURSTSIZE (PORTS_GROUP|all)**

  **port ingress-shaping rate RATELIMIT burst-size BURSTSIZE (PORTS_GROUP|all)**

- Add CLI command to calculate ports rate with a defined time between 10 to 60 Sec.

To start the calculation use:

**show port rate (PORTS-GROUP|all) time (<10-60>)**

To show the last result use:

**show port rate (PORTS-GROUP|all)**

To show the history of the last 5 results:

**show port rate (PORTS-GROUP|all) history**

- L2 protocol tunneling of PVST+ was added.
  **port l2protocol-tunnel (all|cdp|pvst+|stp|vtp) PORTS-GROUP**
- Add CLI command to configure port shaper (ingress and egress) MTU size.
  **port shaper mtu (1536|2048|10240)**
  default = 2048.
- Statistics per port/sl including SNMP support (OaSlStat MIB).
  For details, refer to the application notes.
- LACP can now be configures also on ports and not only trunk ports.
  **port lacp (PORTS-GROUP|all)**
  **port lacp passive (PORTS-GROUP|all)**
- LACP can now be configures to rapid mode to reduce the time to establish LACP session.
  **port rapid-lacp (PORTS-GROUP|all)**
- Access-lists actions of mark vpt, mark dscp and mark sl now support 56 different profiles.
  In previous versions each rule with mark actions allocated an entry from the QoS table even if we used the same values.
- Spanning Tree blocks also loop on a single port.
  The Spanning Tree protocol identify and block the port when a loop is created by connecting the RX & TX on a single port.
- Configure fatal exception parameters. use it to create dump file for debugging in case the device crashes. Default is disabled.
  **exception behaviour (reboot|halt)**
  **exception disable**
  **exception enable**
  **exception memory <1-200>**
  **exception memory unlimited**
- TACACS+ including accounting
  For details, refer to the application notes.
- Radius accounting is supported.
  **accounting commands radius**
  **accounting exec radius**.
- Multiple IPs per interface
  Secondary IP addresses can now be added to interfaces
  The CLI command (in interface node) to add more IP addresses:
  **ip A.B.C.D/M**
- Protocols MAC addresses are enabled in the hardware only when the protocol is enabled in the software.This saves entries in the learning table and the protocols can now be transparent in the device when they are disabled.

- New Scheduler to run linux/CLI commands.Every command has a uniqe Schedule node to simplify and expand configuration.
  `schedule extended <1-65535>`
- Telnet and SSH sessions are limited to 5 (for security reasons).
- Default timeout of the device is 5 minutes.
  We can change the timeout using:
  `exec-timeout current-session <1-35791>`
  `exec-timeout global <1-35791>`
  Or disable the timeout using:
  `no exec-timeout current-session`
  `no exec-timeout global`
- Management rules are now limited to 20 per interface (were 10 in previous versions).
- Support copy current startup configuration to the backup partition.
  `copy startup-config backup-partition`
- New CLI command displays memory usage and processes running in the system.
  `show top-processes`
- Added clock timezone for central europe.
  `clock timezone central-europe.`
- Debugging improvements.
  For details, refer to the application notes.

Version 2.0.11

- Support EM9-CES-E1/ EM9-CES-T1 TDM modules. (1 port CES module).
- Access–List On The Fly.
  Ability to Add, Delete, Modify ACL rules without the need to unbind the ACL first.
  For details, refer to the application notes.
- Binding "extra" ACL to trunk ports.
  `port access-group extra WORD t1`
- Access–List tag nest action can now be binded to port and interface (Not just "extra" ACL).
- Access-List inner-tag and inner-vpt classification for double tag frames.
  `ctag eq <0-4095> [MASK_HEX_VALUE] c-vpt eq <0-7>`

  New profile:

  In order to classify double tag packets we must configure a new ACL double-tag profile using the command:

  `access-list extended-profile (normal|double-tag)`

  Legality:

  - Change profile available when all the ACLs are unbound.
  - The binding process fails when the rule does not match its profile ('ctag'/'c-vpt' with normal profile).
  - ACL with 'ctag'/'c-vpt' can't be bound to an egress port.

  The only difference between the profiles is in regard to Q-in-Q ports:

  normal profile: - 'tag eq' command in the access list matches the customer tag (tag arriving in the packet) double-tag profile: - the 'tag eq' command in the access list matches the q-in-q tag.

- Access-List tag range classification.
  **ctag eq <0-4095> up-to <1-4095>**

  **tag eq <0-4095> up-to <1-4095>**

  This saves ACL rules because it only takes 1 rule in the ACL.

  The parameters must be tag eq x^2 up-to y^2-1 for example:

  **tag eq 0 up-to 15**

  You can also enter the range you want and the software will give you the closest range.

  for example

```
OS910(config-rule)# tag eq 0 up-to 60
Valid closest range is 0 - 63
```

- Policing Mtu CLI command.
  **policing mtu (1536|2048|10240)**

  use this command when working with policer and jumbo frames above 2048 bytes (default value).

  When setting a rate limiter you must configure the commited burst size (cbs) to a larger value than the policer MTU.

- Spanning Tree forwarding decisions based on 802.1ag.
  This will improve convergence time in some scenarios.

  To enable the port forwarding decisions based on 802.1ag use:

  **port PORTS-GROUP oam-based-force-edge**

  We can also filter events from the 802.1ag

  **oam-filter**

- New CLI Command in the spanning tree node to configure the Transmit Hold Count.
  **tx-hold-count <1-10>**

  **tx-hold-count infinite**

- Spanning Tree BPDUs HW Tunneling & Dropping.
  For details, refer to the application notes.

- Support up-to 2 remote syslog servers.
  **rsyslog IPV4_ADDRESS [IPV4_ADDRESS]**

- Flow Control Support. (Using Flow Control will Eliminate the QoS capabilities of the device)
  **port flow-control PORTS-GROUP**

- Show Sfp Params and Show Sfp Diagnostics can now be used also for trunk ports.
- Reverse Link-Reflection.
  The downlink port has reverse link state from the uplink.

  When uplink has link on all the downlink ports are off and when uplinks link goes down all the downlinks links go up.

  **link-reflection uplink PORT downlink PORTS-GROUP reverse-state**

- Buffers Shared can now be disabled.
  **no buffers shared**

- Bandwidth CLI command was added under interface node for L3 protocols.
- Telnet sessions are limited to 10 (for security) and the default timeout changed to 30 minutes.
- Default Ethertype for 802.1ag CCM packets is now 0x8902.
- Scheduler can now run without root password defined.
- Configure fan temperature in Fahrenheit.
  **fan temperature fahrenheit <34-149> <34-149>**
- Show Port was improved for trunk ports. We can see the status of each port in trunk.

```
OS910(config)# show port
PORTS CONFIGURATION
==================
PORT MEDIA      MEDIA_SEL LINK  SPD_SEL     LAN_SPD   DUPL  STATE    SL
----------------------------------------------------------------------
1    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
2    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
3    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
4    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
5    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
6    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
7    TP         COPPER    OFF   AUTO         N/A      N/A   ENABLE   1
8    TP         COPPER    ON    AUTO         1 GBps   FULL  ENABLE   1
t1   ---         ---      ON    AUTO         2 GBps   FULL  ENABLE   1
(9)  SFP+100FX  SFP       ON-F  AUTO         1 GBps   FULL  ENABLE   1
(10) SFP+100FX  SFP       ON-F  AUTO         1 GBps   FULL  ENABLE   1
```

Version 2.0.10

- Support OS910M.
- Support new CES modules for OS910M.
  For details, refer to the application notes.
- Support OS930.
- BPDU tunneling according to tag.
  When receiving tagged BPDUs it is now possible to either drop them or flood them on their vlan.
  The CLI command (in spanning-tree node) to set the forwarding decision for tagged BPDU:
  **port PORTS-GROUP tagged-bpdu rx TAG-LIST (drop|flood)**
- Transmit & Receive tagged BPDUs.
  For interoperability reasons it is sometime necessary to accept and transmit tagged BPDUs.
  The CLI command (in spanning-tree node) to transmit BPDUs with specific tag:
  **port PORTS-GROUP tagged-bpdu tx TAG**
  Note that tagged BPDUs are received and treated now as untagged BPDUs by default.
- VACM.
  For details, refer to the application notes.
- Console disable.
  Access through the serial interface can be disabled to prevent local access to the CLI. Remote access using Telnet/SSH/SNMP still works assuming that the right configuration is set.
  The CLI command to disable the console immediately (should be executed from remote session):

`console-disable`
The CLI command to disable the console in 1 minute:
`console-disable delayed`

- 802.1ag and ITU-Y1731 improvements.
  more services and MEPs support.
- 802.1ag and ITU-Y1731 link trace.
  `mep 1 linktrace rmep 2`
- Scheduler support for all 802.1ag and ITU-Y1731 CLI commands.
  for example:
  `schedule start-time Oct 20 9:20 5 frequency 1 cli ethernet oam domain 1 service 1 mep 1 delay-measure rmep 2 5`
- History of 802.1ag and ITU-Y1731 loopback, delay-measurement and link-trace tests results.
  CLI to configure history size:
  `mep 1 loopback history-size 120`
  `mep 1 delay-measure history-size 120`
  **show history of results:**
  `show loopback history`
  `show delay-measure history`
- Link Protection and Link Reflection based on 802.1ag.(Beta Version).
  For details, refer to the application notes.
- DHCP option 82 support.
- Hash configuration function for Link Aggregation (Trunks).
  Hash function can be configured to be based on physical port or L2 fields (source and destination MACs) or L3 fields (source and dest ip addresses) or L4 fields (TCP and UDP source and destination ports).
  `port trunk mode (l2|l3|l4|port)`
- L2 protocol tunneling of CDP, STP, VTP.
  `port l2protocol-tunnel (all|cdp|stp|vtp) PORTS-GROUP`
- MSTP optimization.
  For details, refer to the application notes.
- Spanning Tree region-expedite.
  For details, refer to the application notes.
- Change buffers profile for ingress direction.
  we can change the buffers size in the ingress direction of a port.
  `port buffers profile <1-7> ingress [PORTS-GROUP]`
- Actions on lt-limit
  Add possibility to drop frames when the number of learned addresses reached the defined limit. Additionally an SNMP trap is sent to indicate that the limit is reached.
  The CLI command to define a drop action for the specified port(s):
  `lt limit action drop (PORTS-GROUP|all)`
- Statistics of L2 protocols such as STP, LACP, 802.3ag.
  `show l2cntrl-protocol-counters`
  `clear l2cntrl-protocol-counters`

Version 2.0.9

- New ACL action to modify the c-tag (customer vlan).
  `tag swap-ctag <VLAN-ID> stag <VLAN-ID>`
- New ACL action for nested vlan.
  `tag nest <VLAN-ID>`
- Egress ACL support with the following actions:
  **permit, deny, mark VPT, mark DSCP, tag swap.**

  `access-list extended ACL_NAME.`

  Binding the ACL to egress port:

  `port access-group egress ACL_NAME PORT_NUMBER.`

  There are a few limitations when configuring Egress ACL:

  - Can only be bounded to port.
  - Can't change port tag-outbound-mode when the port is bounded to egress ACL.
  - ACL can't be bound to ingress and egress at the same time.
  - ACL with mark-vpt/tag-swap should have a default action permit and be bounded to tagged/hybrid port.
  - Mark DSCP action should be configured with ethertype eq 800/86dd rule.
  - Rule with ethertype 0x806 (arp) can't match src/dest IP.
  - Can't classify with L4 (source/destination port).
  - Can't classify with physical source port.
- Add SNMP traps and CLI events for:
  - \- high/normal Temperature.
  - \- Fans on/off.
  - \- Power supply on/off (for OS900 dual AC or dual DC only).
- Support 802.1ag and ITU-Y1731 functions.
  For full details and configuration examples refer to the 'Ethernet Service OAM' application notes.

Version 2.0.8

- Support for classification of source and destination MAC addresses in ACL (for non-ip/arp packets only).
  `src-mac-addr-for-non-ip eq MAC_ADDRESS [MASK]`

  `dst-mac-addr-for-non-ip eq MAC_ADDRESS [MASK]`
- Ability to define redirect action to a trunk port.
  `action redirect port PORT`
- Multiple actions in a single ACL rule.
- Support for BOOTP/TFTP: the switch can take an IP address automatically during boot (DHCP client), and then take the configuration from a remote TFTP server.
  `bootp VLAN-TAG PORTS TAGGED-PORTS get-cfg-via-tftp CFG-FILENAME TFTP-SERVER`. (CLI to configure bootp which gets a dynamic ip from dhcp server and configuration file from the tftp server).

  `bootp VLAN-TAG PORTS TAGGED-PORTS` (CLI to configure bootp which gets a dynamic ip from dhcp server).

`show bootp` (CLI to show BOOTP/DHCP/TFTP configuration).

- LACP (802.3ad) support – link aggregation control protocol.

  `port trunk NAME lacp.` (CLI to configure active lacp trunk).

  `port trunk NAME lacp passive.` (CLI to configure passive lacp trunk).

  `show port lacp.` (CLI to show ports lacp status).

Version 2.0.4

- Routing Features
  - Wirespeed L3 forwarding
  - Routing information Protocol (RIP I & RIP II)
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol (BGP-4)
  - ISIS
  - Static routes
  - Black hole routes
  - Dummy Interfaces
  - Virtual Router Redundency Protocol (VRRP)
  - IP NAT (note that this is a software NAT with limitied performance)
- New Linux kernel 2.6.15
- Ingress scheduling configuration was added: port priority-queuing profile can be assigned to a port in it's ingress phase (previous versions had this feature on egress only). This features enables applications like per access port ingress scheduling (e.g.using wrr to enable differnet trafic shares per service-level, doing that on a per customer/access-port basis).
- A new port mode was added: 'untagged-multi-vlans'. This new mode, in combination with the 'tag swap' action in the ACL, enables applications like protocol based VLANs, and the usage of the out-of-band port for performing software-based routing and NAT.

Version 1.0.9

- Added support for the OS912 device.
- Improved support for fan and power-supply status reporting.
- Added two new combined ACL actions: action-list+mark+swap-vlan, mark+swap-vlan.
- Added classification of the source physical port in ACL rules (can be usefull in access-lists binded to a vlan, having different treatment for different ingress ports within the same vlan).
- Protected-ports: for each source port define the allowed destination ports, overiding other forwarding decisions in order to support port level security.
- Added option to configure priority queuing for a trunk port: the queuing itself is still on each port but the queuing configuration is copied internaly for all ports of the trunk.
- Improved performance for link-protection when returning to the primary link uppon it's recovery.
- Flood limit: more accurate limit and an 'extra' flood limit option that enables definition of two flood rates (with differnet traffic types) for the same ingress port.

- RADIUS support for direct login into enabled mode: such a login is enabled when a user is configured on the RADIUS server with the attribute ‘Service-Type’ set to ‘Administrative-User’.

Version 1.0.6

- Support for two sets of egress counters (version 1.0.3 have only one), and two sets of ingress counters.
- Classification of Ethertype field in ACL rules (matches the first non-vlan ethertype).
- Mirroring per ingress vlan.
- Improvements in the default configuration of memory buffers and descriptors budgets.
- Auto operation of the fan (can set the on and off temperatures).
- Dropping of Broadcast and Multicast packets for IPv6,IPv4 and non-IP packets per ingress vlan.
- SA-MAC and DA-MAC actions (drop, fwd) per LT entry: ability to drop packets based on their source or destination MAC address.
- Support for tc-group-mib (per flow accounting).

Version 1.0.3

- First software release.