NOKIA
CONNECTING PEOPLE

Nokia

ESB26 GigabitEthernet Switch

User Guide

Document History

ISSUE	DATE ISSUED	COMMENTS
MN700004 Rev 01	15 Jan 2004	First draft.

Table of Contents

Preface

This guide provides the required information to setup and configure the ESB26 switch, *firmware version 3.3.0*. It is intended for network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of the following:

- Local area networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- Internet Protocol (IP) concepts

If the information in the Release Notes that are shipped with your unit differs from the information in this guide, follow the Release Notes.

Conventions Used in This Guide

The syntax of CLI command lines, explained in "Basic CLI Operating Conventions" and the further topics and discussed throughout this guide, is represented by the following general format:

```
device-name>keyword(s) [parameter(s)] ... [keyword(s)] [parameter(s)]
```

OR

```
device-name[ (config ...)]#keyword(s) [parameter(s)]
                           ... [keyword(s)] [parameter(s)]
```

where:

- The angle bracket (>) is the CLI prompt symbol in View mode.
- The pound symbol (#) is the CLI prompt symbol in all other modes.
- The left part, up to and including the prompt symbol represents the command prompt displayed by the computer. In this part:
  - *device-name* stands for the name of the switch (e.g. ESB26).
  - The optional expression “(config)” or “(cfg ...)” – including the parentheses – appears on the screen exactly as in the manual.
  - The part following the prompt symbol represents the users command. In this

part:

> **keyword(s)**, in **boldface** characters, stands for one or more standard CLI command keywords. The first keyword may optionally be preceded by **no** to indicate a negation of the command.

> *parameter(s)* may be one or more optional or requisite values, depending on the requirements of the specific command. They are represented by *slanted characters*.

> In this guide, keywords and parameters may be separated by vertical OR bars (|). The OR bars indicate an exclusive-or choice among a group of selectable entities separated by these symbols.

> Parentheses and braces may be used in this guide to enclose selectable entities – for the purpose of clarification.

Acronyms Used in This Guide

L3	OSI Layer 3 requirements
DHCP	Dynamic host configuration protocol
Downlink	The Ethernet links connecting to equipment that perform host data processing.
GARP	Generic Attribute Registration Protocol
GMRP	Group Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
MAC	Media Access Control
MIB	Management information base
pps	Packets per second
SNMP	Simple network management protocol
STP	Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol
Uplink	The Ethernet links connecting to another switch or router.
UTP	Unshielded twisted pair
VLAN	Virtual Local Area Network
10Base-T	10Mbit/s Ethernet link that works over standard UTP copper cabling.

100Base-TX	100Mbit/s Ethernet link that works over standard UTP copper cabling.
1000Base-T	1000Mbit/s Ethernet link that works over standard UTP copper cabling.
1000Base-SX	1000Mbit/s Ethernet link that works over optical, 850nm multimode cabling.

Summary of Version 3.3.0 Features

The Version 3.3.0 includes the following features:

- VLANs (Virtual local area networks) including support for IEEE 802.1Q and IEEE 802.1p
- VLAN aggregation
- STP (Spanning Tree Protocol) (IEEE 802.1D)
- RSTP (Rapid Spanning Tree Protocol) (IEEE 802.1w)
- MSTP (Multiple Spanning Tree Protocol) (IEEE 802.1s)
- QoS (Quality of Service)
- IGMP snooping to control IP multicast traffic.
- GMRP (GARP Multicast Registration Protocol)
- GVRP (GARP VLAN Registration Protocol)
- MVR (Multicast VLAN Registration)
- Console CLI (Command-line Interface) connection
- Telnet CLI connection
- SNMP (Simple Network Management Protocol) v1, v2c and v3 support
- RMON (Remote Monitoring)
- Traffic mirroring for all ports
- DHCP Client
- Backpressure and flow control support
- 802.3x flow control for full-duplex links
- Link Aggregation (LAG) for increased bandwidth without requiring expensive hardware upgrade
- Link Aggregation Control Protocol (LACP) providing dynamic LAGs
- Console timeout value
- Remote logging
- Remote time synchronization protocol (rfc867, rfc868).
- SSH

- RADIUS
- CLI user privilege levels
- Resilient link for port redundancy
- Script file system
- Up to 1.7 MB size of the configuration file
- More accurate CPU utilization measurement
- Inform requests for SNMPv2c
- MAC address per port in BPDU for xSTP
- Enhanced DHCP boot process:
    - Startup configuration integrity check
    - Option to save downloaded file to the internal Flash memory
- Image file upload
- Enhanced password security (passwords are saved in the internal Flash memory and not in the running config, startup or script files.)
- Cable crossover support

1. Introduction

Overview

ESB26 is an integrated Ethernet switch based on DX200 hardware platform. The ESB26 features a total of 26 Ethernet ports of types and placements as follows:

Port	Placement	Connector	Traffic
20 full duplex 10/100Base T/TX Ethernet ports	back panel	AMP 2mm Z-pack connectors compatible	downlink
2 full duplex 10/100Base T/TX Ethernet ports	front panel	RJ45	downlink/uplink
2 1000Base-T ports	front panel	RJ45	downlink/uplink
2 1000Base-SX ports	front panel	LC	uplink

ESB26 contains also one RS-232 interface (RJ45) on the front panel for management purposes.

The two 1000Base-T ports support all the 10/100/1000 Mbit/s link speeds. Speed mixing is supported, too, e.g. it is possible to use one of the 1000Base-T ports in gigabit mode while the other runs in 100Mbit mode.

The intended use of the ESB26 is to collect the Ethernet links of different computer units and preprocessor units of DX200-based network elements, and allow access to them from the upper levels. The ESB26 can be used in all M98F DX200 based network elements. The ESB26 can be assembled into a place of ESB20/ESB20-A by using the existing cabling.

NOTE The ESB26 is designed to operate in forced cooling M98F only.

The two graphics below represent two examples of operational environments for the ESB26. As presented, the ESB26s are used to collect traffic from/to different computer units and preprocessor units and forward it towards 3rd party L3 switches. It is important to note that VLAN-technology is used in order to divide the different units into several broadcast domains. It must also be noted that redundant paths do exists and Rapid STP (as according to IEEE 802.1w) is used in order to avoid loops.

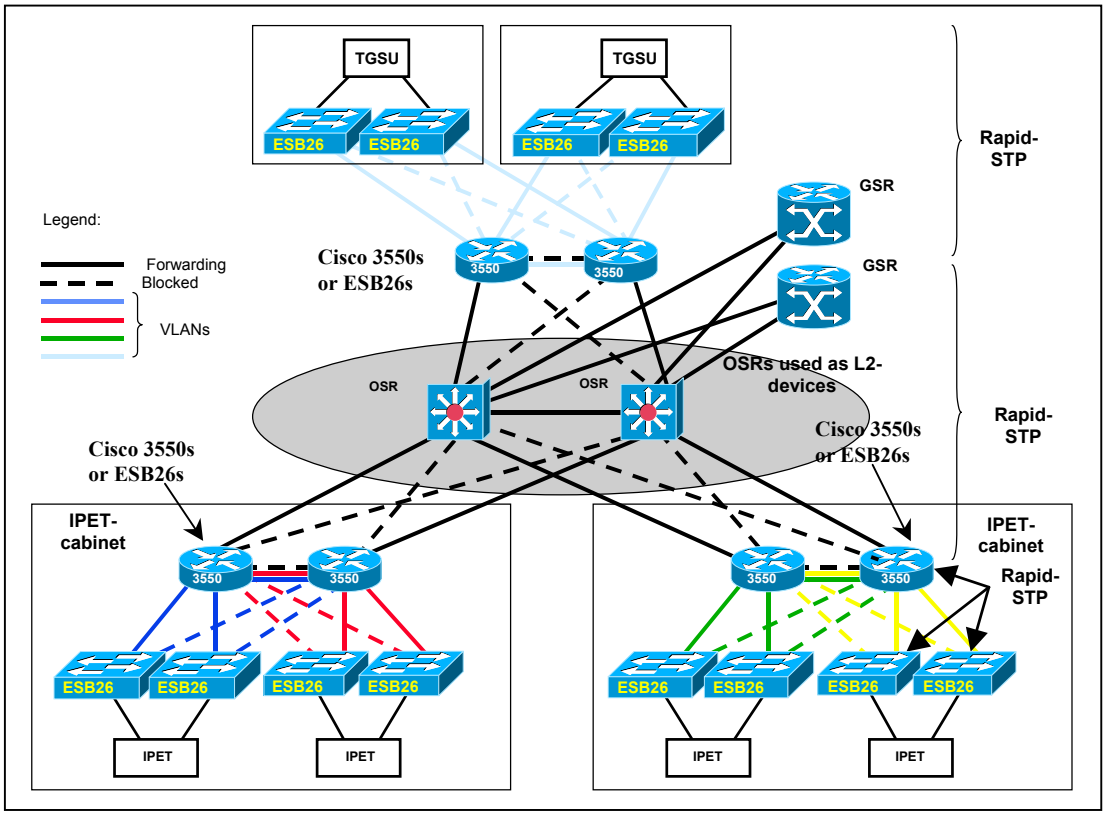


Figure 1-1 Example of Operational Environment for the ESB26 with L2 OSRs

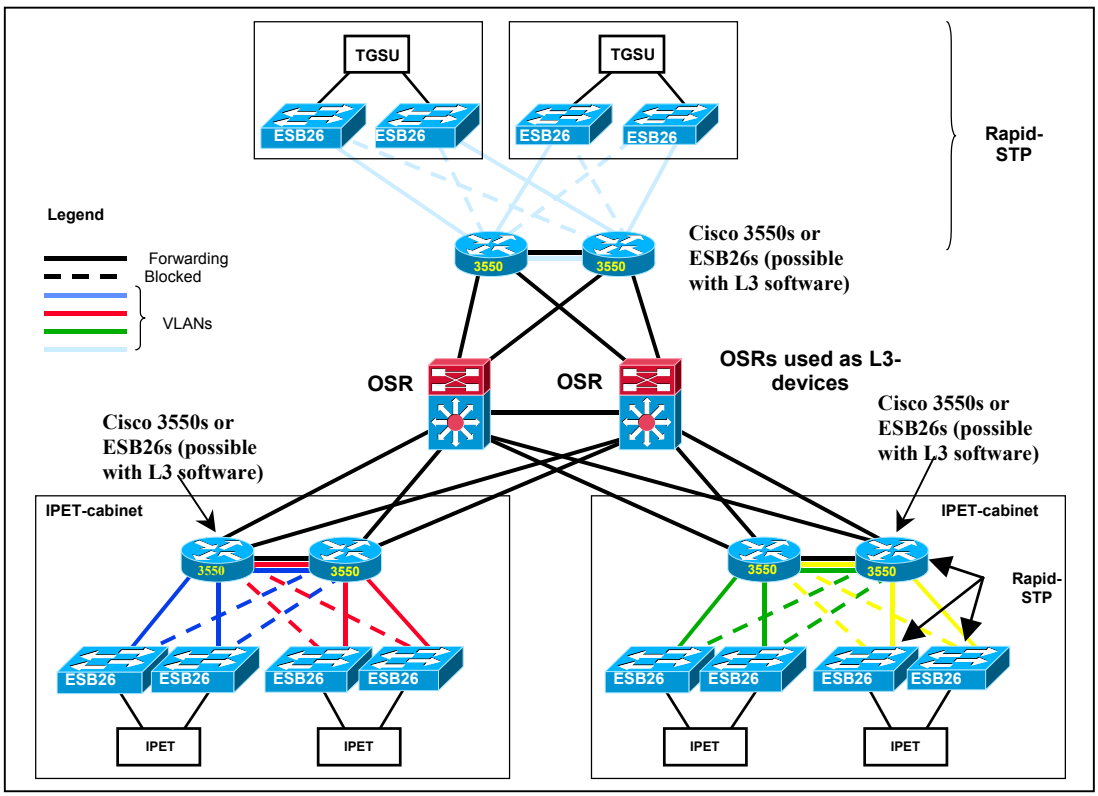


Figure 1-2 Example of Operational Environment for the ESB26 with L3 OSRs.

The switch is managed via BiNOS™ Command Language Interface (CLI) commands typed in by the user by either of the following means:

- By direct connection, through a VT-100 compatible terminal connected to the console port on the unit's front panel;
- Remotely, using telnet over a TCP/IP communication network.

Specifications

Compliance

- IEEE802.3
- IEEE802.1d
- IEEE802.3X
- IEEE802.1q
- IEEE802.1w
- IEEE802.1s
- IEEE802.3ad

Switching Characteristics

Bridging	Per IEEE 802.1d / 802.1w /802.1s spanning tree.
Address table:	16 K MAC address per switch.
Forwarding Rate:	148,800 packets-per-second maximum for 100Base ports.
Internal Bandwidth (max):	1,488,000 packets-per-second maximum for 1000Base ports.
Buffers Memory:	5.3 Gbps (Full Duplex).
Priority Queuing:	32 Mbytes
Virtual LAN:	8 Queues per port, provides CoS per 802.1p Port Based VLAN per 802.1q. Up to 4094 VLAN groups can be defined. GVRP protocol support.
Port Aggregation:	Up to 7 static or dynamic LAGs can be defined.
In-Band:	SNMP, TELNET,
Supported MIBs:	MIB-II, BRIDGE MIB (RFC-1493), PRIVATE MIB, RMON MIB (Group I,2,3,9)

Local:	For initial configuration, EIA-232 protocol, RJ-45 console connector on the front panel, VT100 compatible

Management

Software download:	Via TFTP (Server application)
Monitoring:	Port mirroring for sniffer connection.
Max. configuration file size:	1.7 MB

Indicators

General:	Operation Indicator. A single two-color LED (Green/Red) • Green: the unit is operational. • Red: during power up and in faulty condition. • Blinking orange: when no image software is loaded. • Off: power is off.

Physical Characteristics

Dimensions:	233.4x220mm with PCB thickness of 1.6mm and spacing of 20.34mm (4T)
Supported chassis models:	CC3C-ACC4C-ACM2C-ALASWC-AIPETC-A

Environmental Characteristics

Operating Temperature:	According to Nokia Environmental Specification (Commercial Range 0-70°C)
Humidity:	Complying to Nokia Environmental Specification

Power Characteristics

Voltage:	+3.3Vand +5V (±5% voltage tolerances)
Power Consumption:	Less than 25 W

Ex-Factory Default Settings

IP Address:	192.168.0.5

Subnet mask:	255.255.255.128
Default gateway:	192.168.0.10
Password:	***nokia***
Telnet:	enabled
SNMP:	disabled
RMON:	enabled
802.1p priority recognition:	enabled
802.1q tagging:	disabled on the default VLAN
Forwarding database aging period:	300 seconds (5 minutes)
GVRP:	disabled
GMRP:	disabled
SSH:	disabled
LACP:	disabled
LAN ports status:	enabled
Port auto negotiation:	enabled
Port mirroring:	disabled
VLANs:	disabled
Rapid STP:	disabled
DHCP:	enabled

Hot-Swap

The card can be inserted and removed while power is applied to the IPA2800 chassis. Before removing the card, press the **Reset** button twice within two seconds. This will disconnect power from the card for 20 seconds. The LED will turn off, indicating that the card can be safely removed.

2. Getting Started

Overview

ESB26 installation consists of inserting the card into the appropriate slot in the system, turning the unit power on, and setting the IP Address in order to enable remote management. All other management procedures may be performed remotely via Terminal Interface management applications that are integrated into the unit.

This chapter describes how to install the unit, perform initial setup, use Terminal Interface management applications, and how to perform basic switch operations.

Unpacking

After unpacking:

- Verify that the ESB26 unit has not been damaged during shipment.
- It is recommended that you keep the shipping package until the unit has been installed and verified as being fully operational. As all electronic devices with static sensitive components, ESB26 should be handled with care.

Front Panel

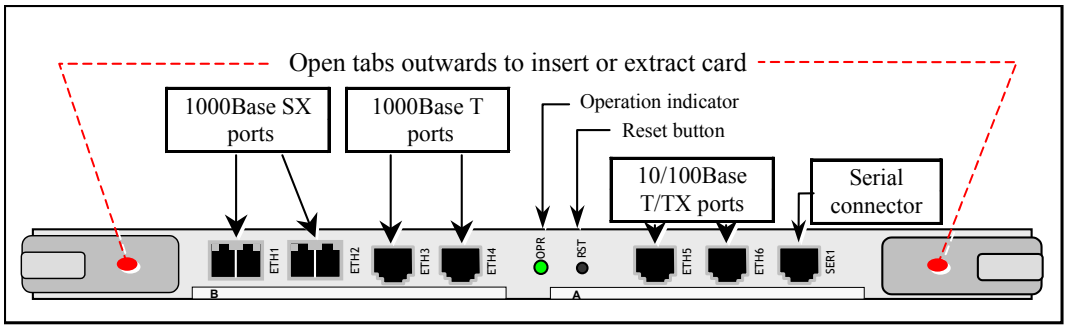


Figure 2-1 ESB26 Front Panel

Table 2-1 ESB26 Front Panel Components

ETH1, ETH2	Two 1000Base SX ports interface connectors

ETH3, ETH4	Two 1000Base T ports interface connectors
ETH5, ETH6	Two 10/100Base T/TX ports interface connectors
OPR	Operation Indicator. A single two-color LED (Green/Red) • Green: the unit is operational • Red: during power up and in faulty condition. • Blinking orange: when no image software is loaded. • Off: power is off.
RST	Local Reset and Hotswap button. To perform Hotswap, press twice within two seconds before removing the card. Power will be turned off for 20 seconds during which the card may be removed safely.
SER1	RJ45 console connector used for initial configuration. TX – Pin 2 (Going out of the switch) RX – Pin 5 (Going into the switch) GND – Pin 3 GND – Pin 4

Using the CLI to Configure the Switch

The configuration program uses a CLI (Command Line Interface) that enables you to start using the switch quickly and without extensive background knowledge. It does this by prompting you for the information required to perform basic configuration procedures.

Using the CLI, you will be able to do the following:

- Establish host names and interfaces
- Enable transparent Ethernet bridging
- Configure Layer 2 switch protocols (GVRP, GMRP, Spanning Tree, etc.)
- Configure VLANs

System parameters are stored in a non-volatile memory. They have to be set up only once during initial setup.

Getting Started with the CLI

Configuration of the switch is done by connecting a VT-100 (or compatible terminal) to the card RJ-45 (Console) connector.

The CLI operates automatically when you power on the switch. Before you start using the CLI, you must do the following:

Step 1. Insert the device into its chassis slot.

Step 2. Attach an RS-232 ASCII terminal to the RJ-45 (SER1) connector (See Figure 2-1).

Step 3. Configure the terminal to operate at:

- Emulation mode: VT-100 mode (default mode)
- 9600 bps
- 8 data bits
- 1 stop bit
- No parity
- No flow control

25 lines and 80 columns window size

Step 4. Establish a session with the unit and power on the unit. After a few seconds, the following is displayed on the terminal screen:

```
Press any key to stop auto-boot...
 0

Verifying validity of primary application.....OK



Start primary application...

BUILT-IN SELF TEST
------------------
CPU Core Test        : Passed
CPU Notify RAM Test  : Passed
CPU Interface Test   : Passed
Testing Switch Core  : Passed
On-board Power Test  : Passed




////////////////////////////////////////////////////////////////////////
//                                                                    //
//              N O K I A                                             //
//                                                                    //
//                                                                    //
//  Switch model : NOKIA ESB26                                        //
//  SW version   : 3.2.89 ER created Dec 17 2003 - 11:32:40           //
//                                                                    //
////////////////////////////////////////////////////////////////////////



User Access Verification

Password:
```

Step 5. Enter your password, which is ***nokia*** by default. The device-name> prompt is displayed, allowing you to begin the configuration process.

If the password has been lost or cannot be configured, please contact Nokia support.

Planning the Configuration

Before starting the configuration process, determine the following:

- The protocols you plan to use and their specific parameters
- The types of interfaces installed: Ethernet or Serial
- Whether or not you plan to use bridging

Basic CLI Operating Conventions

Entering commands at the CLI prompt and then pressing the Return key initiates CLI commands. Based on user input, the CLI returns various data in response.

You type all commands on one line and then press <Enter>. The CLI response is displayed on your screen.

You can use abbreviated commands provided they are unique. For example, enter the letters **sho** for the **show** command.

Certain commands display multiple screens with this prompt at the bottom of the screen:

```
--More--
```

Press on the space bar to continue.

Special Keys

Table 2-2 summarizes special keys available at the CLI prompt.

Table 2-2 CLI Entry Keys

Key	Action
Backspace	Erase characters
Ctrl-U	Delete line
Ctrl-W	Erase the last word
Exit	Escape current mode and go to previous mode

Key	Action
Ctrl-F	Move forward one character
Ctrl-B	Move backward one character
Esc and then B	Move bacward one word
Esc and then F	Move forward one word
Ctrl-A	Move to the beginning of the line
Ctrl-E	Move to the end of the line
Ctrl-H	Delete the character before point
Ctrl-D	Delete the character after point
Esc and then D	Forward kill word
Ctrl-K	Kill to the end of the line
Ctrl-C	Interrupt current input and moves to the next line
Ctrl-N	Move down to next line in the history buffer
Ctrl-P	Move up to previous line in the history buffer
Tab	Use command line completion by pressing the Tab key.
?	Typing ? at the beginning of the line, generates a list of available commands. Typing ? at any point within the line will show possible completions.

CLI Modes

There are several CLI modes and associated prompt levels. The prompt is the string that appears after the host name (ESB26 by default). The following are the main CLI modes:

View Mode (user-level)

The View mode allows viewing capabilities only. Its prompt is an angle bracket (>):

```
device-name>
```

View mode is password protected. The password is ***nokia*** by default. You can change this password by using the **password** command in global Configuration mode.

Privileged Mode

The Privileged mode allows advanced viewing unit capabilities and limited configuration capabilities. Its prompt is a pound symbol (#):

```
device-name#
```

By default, Privileged mode is not password protected. However, you can configure password protection by using the **password** command from the Configure prompt.

To access Privileged mode from View mode, use the **enable** command. (That is why this mode is also referred as "Enable" mode.)

Configure Mode

The Configure mode allows full configuration capabilities. Its prompt is displayed as follows:

```
device-name(config)#
```

Additional information can be displayed inside the parentheses, before the pound symbol, to indicate the present configuration mode.

For example:

```
device-name(cfg protocol)#
```

indicates that you are in the Configure Protocol mode.

To access Configure mode from Privileged mode, use the **configure terminal** command.

Startup Modes

There are also two separate special startup modes, called "Loader" and "Sysloader". They are designed mainly for techical support purposes and are not user-configurable. Both of them are covered in detail in the Appendix.

Messages

Several messages may be issued in response to incorrect entries (e.g., wrong syntax, or incomplete commands). The following are some of these messages:

```
% unknown command
```

displayed when you enter a string that is not a command.

```
% command incomplete
```

indicates that you entered a valid command but failed to enter all its required parameters. Press the <Tab> key to display the possible options.

Other messages include:

```
% ambiguous command.
% port 9 invalid, valid val: 1..8
```

Getting System Help

For system help, enter **?** or the letter **l** (for "list") to display a list of commands that are available at either the user-level or the privileged-level CLI prompt.

To get more information about certain commands, type **?** after the command. For more information, see the lists of commands that are displayed after entering **?**

Using the List Command

The **list** command displays a complete list of the commands relevant to the prompt displayed. If the list is larger than can be displayed on your screen, the following is displayed.

```
--more--
```

Command History

A memory buffer in the ESB26 retains the last 20 commands you entered.

Using Telnet

Any workstation with a telnet facility should be able to communicate with the ESB26 over a TCP/IP network. Up to five active telnet sessions can access the ESB26 concurrently. The telnet session will be disconnected after a specified time of inactivity.

Before you can start a telnet session, you must set up the IP parameters described in the Configuring the Device's IP Parameters section. Telnet is enabled by default.

To open the telnet session, you must specify the IP address of the device that you want to manage. Check the user manual supplied with the telnet facility if you are unsure of how to do this.

Once the connection is established, you will be prompted to log in. VT100 emulation and VT100 keys must be used.

Configuring the Device's IP Parameters

To manage the ESB26 by a telnet connection or by using an SNMP Network Manager, you must first configure the IP parameters of the ESB26 switch and the default gateway.

Step 1. Change to Global Configuration mode by typing **configure terminal** at the Privileged mode prompt.

The DHCP client is enabled by default; therefore, to configure a static IP address, you should first disable the DHCP client.

Step 2. To disable the DHCP client, use the following command in Global Configuration mode:

Command Syntax

```
device-name(config)#no ip address dhcp
```

Step 3. To set the IP address, use the following command in Global Configuration mode:

Command Syntax

```
device-name(config)#ip address A1.B1.C1.D1 [/M|A2.B2.C2.D2] [dhcp
A3.B3.C3.D3]
```

Argument Description

A1.B1.C1.D1	IP address of the configured IP interface.
/M	Subnet mask of the configured IP interface (in the range 1-30).
A2.B2.C2.D2	Subnet mask of the configured IP interface.
dhcp	Use dhcp client
A3.B3.C3.D3	Request IP address A.B.C.D

Example

```
device-name(config)#ip address 100.1.2.3/16
device-name(config)#ip address dhcp 9.0.0.1
```

The IP address of the ESB26 becomes 100.1.2.3 in network 100.1.0.0

Step 4. Set the default gateway IP address as follows:

Command Syntax

```
device-name(config)#ip route {destination-address
netmask|destination-prefix} A.B.C.D [<distance>]
device-name(config)#no ip route {destination-address
netmask|destination-prefix} A.B.C.D [<distance>]
```

Argument Description

destination-address	Route's IP destination address, in A.B.C.D format, used in conjunction with netmask to define a network address.
netmask	Destination network mask, in A.B.C.D format, used in conjunction with destination-address.
destination-prefix	Route's destination prefix, in A.B.C.D/M format.
A.B.C.D	IP gateway address in A.B.C.D format.
distance	(Optional). Distance assigned for this route, in the range <1-255>.

Example

```
device-name(config)#ip route 0.0.0.0/0 100.1.1.1
```

The default gateway IP address is 100.1.1.1 in network 100.1.0.0

General Commands

Table 2-3 shows the commands you can use at all times, regardless of the type of prompt displayed.

Table 2-3 General Commands

exit	Escape current mode and go to previous mode
help	Display help information
no	Negate a command or set its defaults
quit	Escape current mode and go to previous mode

View Mode and Privileged Mode

Table 2-4 summarizes the Privileged mode commands. The **enable** command is available only in View mode and is used to access Privileged mode. All other commands listed in the table are available in Privileged mode. The **show** command and the **terminal** command are available both in View and in Privileged mode.

Table 2-4 Privileged Mode Command Summary

clear	Clears a specified entry or entries from one of the tables (the command is available only in Privileged mode).
configure	Configuration from VTY interface (the command is available only in Privileged mode).
copy	Transfers file to the target base (the command is available only in Privileged mode).
debug	Enables the debugging options
disable	Exits from Privileged mode (the command is available only in Privileged mode).
enable	Enters Privileged mode (the command is available only in View mode).
reload	Halts and performs a cold restart (the command is available only in Privileged mode).
self-test	Shows built-in test results (the command is available only in Privileged mode).
session	Telnet session commands (the command is available only in Privileged mode).
show	Shows running system information.
telnet	Start telnet client (the command is available only in Privileged mode).
terminal	Terminal configuration setup.
ping	Sends ICMP echo messages (the command is available only in Privileged mode).
traceroute	Trace routing path (the command is available only in Privileged mode).
who	Displays who is on VTY.
write	Writes configuration to memory, network or terminal (the command is available only in Privileged mode).
scp-image	Secure copy.
swap	Swaps the primaryand the secondary applications.

Accessing Privileged Mode

enable

The **enable** command, in View mode, allows accessing the Privileged mode. After entering this command, the prompt symbol changes from an angle bracket to a pound symbol (#).

Command Syntax

```
device-name>enable
```

Example

```
device-name>enable
device-name#
```

Description of View and Privileged Mode Commands

configure terminal

The **configure terminal** command, in Privileged (Enable) mode, allows accessing the Global Configure mode, for configuration of VLANs, interfaces, resilient link, etc.

Command Syntax

```
device-name#configure terminal
```

Example

```
device-name#configure terminal
device-name(config)#
```

terminal length

The **terminal length** command, in View or Privileged (Enable) mode, specifies the number of lines the CLI displays, in response to a command, before displaying the `--More--` string.

Command Syntax

```
device-name#terminal length
```

show ip

The **show ip** command, in View or Privileged (Enable) mode, displays the IP address of the ESB26 and its subnet mask.

Command Syntax

```
device-name#show ip
```

Example

```
device-name#show ip
IP-ADDR : 212.29.220.136 NET-MASK : 255.255.255.192
device-name#
```

show ip arp

The **show ip arp** command, in View or Privileged (Enable) mode, displays Address Resolution Protocol information.

Command Syntax

```
device-name#show ip arp
```

Example

```
device-name#show ip arp
show ip arp
======+==================+================+========+========+
   #  |   IP Address     |     MAC        |Age(min)|   if   |
```

```
----0-|------192.168.0.4 |00:40:95:30:12:2e|----2---|---sw0--|
    1 |     192.168.0.22 |00:40:95:32:76:04|    1   |   sw0  |
    2 |     192.168.0.44 |00:40:95:30:5e:e1|    1   |   sw0  |
device-name#
```

traceroute

The **traceroute** command, in Privileged (Enable) mode, displays the routing path from the ESB26 to the targeted IP address. This command can help determine how routing is done in the network. The execution of the command can be stopped by pressing the ESC key.

Command Syntax

```
device-name#traceroute A.B.C.D [TTL] [TIMEOUT]
```

Argument Description

A.B.C.D	The IP address to be traced.
TTL	Defines the numbers of routers that allow the traceroute command to pass when it looks for the specified IP address.
TIMEOUT	Defines the length of time (in seconds) that an answer to a traceroute request can be received (default is 2 seconds).

ping

The **ping** command, in Privileged (Enable) mode, allows to ping a unit.

Command Syntax

```
device-name#ping A.B.C.D [NUMBER] [TIMEOUT] [DELAY] [LENGTH]
```

Argument Description

A.B.C.D	The destination IP address.
NUMBER	Number of echo packets to send (default 5).
TIMEOUT	Wait for response in seconds (default 2 seconds).
DELAY	Delay between packets in seconds (default immediately).
LENGTH	Size of the ICMP echo packet (default 100).

Example

To send 5 pings of 80 bytes with a 30-second wait for reply and a 20-second delay between pings, enter the following command:

```
device-name#ping 212.29.220.136 5 30 20 80
sending 5, 80-byte icmp echos to 212.29.220.136, timeout is 1 seconds: !!!
```

The exclamation points are displayed at the end of each successful packet. The CLI prompt is displayed on your screen when the entire ping sequence has been completed. The execution of the command can be stopped by pressing the ESC key.

Configure Mode

The Configure mode allows full configuration capabilities. Its prompt is as follows:

```
device-name(config)#
```

Additional information can be displayed inside the parentheses, before the pound symbol, to indicate the present Configuration Mode.

For example:

```
device-name(cfg protocol)#
```

indicates that you are in the Configure Protocol mode.

Accessing Global Configuration Mode

To access Global Configuration mode:

Step 1. Type the **enable** command at the EXEC prompt:

```
device-name>enable
```

The prompt indicates entry into Privileged mode:

```
device-name#
```

Step 2. Type **configure terminal** at the Privileged-level prompt. The prompt following this command indicates entry into the global Configuration mode.

```
device-name(config)#
```

Configuration Command Types

Configuration commands are categorized as follows:

Global configuration commands	Defines system-wide parameters.
Interface configuration commands	Defines the characteristics of an interface (for example, a Serial or Ethernet interface). To access these commands, use the interface command in global Configuration mode.
Line subcommands	Defines the characteristics of a serial line. These commands must be preceded by a line command.

Observe the following guidelines when you execute configuration commands:

- You can enter configuration subcommands in uppercase letters, lowercase letters, or both. You can also abbreviate all commands and other keywords to the least number of characters that uniquely identify the command.
- To add a comment, begin the line with an exclamation point (!). Comments do not affect command processing.

Configuration Mode Sub-Modes

Configuration mode has several sub-modes, each used to configure various entities in the ESB26. Each mode has its own unique prompt and list of commands. The following are the Configuration mode sub-modes.

Table 2-5 Configure Mode Sub-Modes Summary

Mode	**Description**	**Prompt** (following device-name)
Line VTY Configuration	Configures the VTY sub-mode, to allow accessing the ESB26 via telnet.	`(config-VTY)#`
Interface Configuration	Configures interface ports or port groups.	`(config-if 1/1/1)#` or `(config-if-group)#`
VLAN Configuration	Configures Virtual LANs (VLANs).	`(config vlan)#`
Protocol Configuration	Configures protocols.	`(cfg protocol)#`
Resilient Link Configuration	Configures resilient links.	`(config-resil-link N)#`
File system Configuration	For script file system management.	`(config script-file-system)#`
Monitor Configuration	Configures monitoring parameters.	`(config monitor NAME)#`

3. Configuring a Telnet Connection

Introduction

The telnet protocol is designed to provide a general, bi-directional, eight-bit byte-oriented communications facility. Its primary goal is to allow a standard method of interfacing between terminal devices and terminal-oriented processes. It is envisioned that the protocol may also be used for terminal-terminal communication ("linking") and process-process communication (distributed computation).

A telnet connection is a Transmission Control Protocol (TCP) connection used to transmit data with interspersed telnet control information.

Any workstation with a telnet facility should be able to communicate with the switch over a TCP/IP network. Up to five active telnet sessions can access the switch concurrently. If timeout is enabled, the telnet session will expire after 10 minutes of inactivity. In addition, you can use telnet from the switch to access other devices in the network.

To open the telnet session, you must specify the IP address of the device that you want to manage (For more information, see Configuring the Device's IP Parameters).

Once the connection is established, you will be prompted to log in. VT100 emulation and VT100 keys must be used. Any workstation with a telnet facility should be able to communicate with the switch over a TCP/IP network.

Configuring a Telnet Session

Table 3-1 shows the telnet configuration and related commands.

Table 3-1 Telnet Configuration and Related Commands

Command	Description
telnet	Initiates a telnet client's connection to a specified remote host.
session	Displays the session indexes of all the open sessions.
session kill	Closes the specified telnet connection to the remote host.
who	Displays the currently open telnet sessions on the switch.
telnet	Disables or enables telnet connections to the switch.
line vty	Accesses VTY configuration mode.
exec-timeout	Sets the VTY connection-timeout value.

Description of Commands

telnet

The **telnet** command, in Privileged (Enable) mode, initiates a telnet client's connection to the specified remote host.

If the TCP port number is not specified, the telnet session default port number is 23.

To see the open telnet connections, use the **session** command in Privileged (Enable) mode.

Use the **log telnet-console** command, in Global Configuration mode, to direct log output (messages issued by the system) to the telnet console.

Command Syntax

```
device-name#telnet A.B.C.D [PORT]
```

Argument Description

A.B.C.D	The IP address of the remote host.
PORT	(Optional) The port at which the remote service is running, in range <1-65535>. The default value for telnet service is 23.

session

The **session** command, in Privileged (Enable) mode, displays the session indexes of all the open sessions.

The session number can be used for terminating the session.

Command Syntax

```
device-name#session
```

Example

```
device-name#session
your current session is: 2
available sessions for operating with are: 2
```

session kill

The **session kill** command, in Privileged (Enable) mode, closes the appropriate session to the remote host.

After executing the command, the BiNOS checks if the user is not trying to terminate the master session (the VTY from which other sessions originate). If the result is negative, the command closes the specified session to the remote host.

If the session is terminated, the user with the telnet connection is notified that the session has been terminated.

To view the open sessions, use the **session** command without arguments in Privileged (Enable) mode.

Command Syntax

```
device-name#session kill <session-number>
```

Argument Description

session-number	The session number in range <1-101>.

who

The **who** command, in View or Privileged (Enable) mode, displays the currently open connections to the switch.

The following session types will be displayed:

- Console
- Telnet
- SSH
- RADIUS

Command Syntax

```
device-name#who
```

Example

```
device-name#who
Codes: > - current session, * - configuring
  vty on console connected on console.
   >vty on telnet [1] connected from 10.2.71.137.
```

telnet

The **telnet** command, in Global Configuration mode, disables or enables telnet connections to the switch.

The **stop** parameter disables all telnet connections to the switch. Any telnet connections that are open when this command is executed will be terminated immediately.

To re-enable telnet to the switch, use the **start** parameter.

By default, telnet services are enabled on the switch.

Command Syntax

```
device-name(config)#telnet {start|stop}
```

Argument Description

start	Enables telnet connection to the switch.
stop	Disables telnet connection to the switch.

line vty

The **line vty** command, in Global Configuration mode, accesses VTY (Virtual Telnet Type) configuration mode.

The VTY mode enables you to control the VTY connection to the switch.

The prompt-line *device-name*(config-vty)# that follows the command indicates that VTY configuration mode has been entered.

Command Syntax

```
device-name(config)#line vty
device-name(config-vty)#
```

exec-timeout

The **exec-timeout** command, in VTY Configuration mode, sets the VTY connection-timeout value. The switch logs out when the connection-timeout time expires.

The default timeout value is 10 minutes. A timeout value of zero disables timeout-disconnection (equivalent to unlimited).

The **no** form of this command restores the default 10 minutes timeout value.

If the command is configured without parameters it will display the current timeout value.

Command Syntax

```
device-name(config-vty)#exec-timeout [<minutes> [<seconds>]| unlimited]
device-name(config-vty)#no exec-timeout
```

Argument Description

minutes	The timeout value in the range of <0-35791> minutes.
seconds	Addition of seconds to the timeout value that was defined in minutes in range of <0-2147483> seconds.
unlimited	Sets timeout value to be unlimited.

Example

```
device-name(config-vty)#exec-timeout 3
device-name(config-vty)#exec-timeout
exec-timeout 3 min 0 sec
```

Switching Between Sessions

The user can switch between sessions initiated from the same VTY by pressing **<Ctrl+Shift+*SESSION-NUMBER*>** or **<Ctrl+]>.**

Example

```
device-name#telnet 192.0.103.13

connecting to 192.0.103.13...

current session is 6.

red hat linux release 7.1 (seawolf)
kernel 2.4.2-2 on an i686
login: xxxx
password:
last login: thu mar  7 11:20:42 from 192.0.103.1
[xxxx@io xxxx]$
...
...
device-name(config)#<ctrl+shift+4>
choose session to switch to:
the current session is 4
your sessions are 4 >
```

4. User Privilege Levels

Introduction

The ESB26 Command Line Interface (CLI) supports privilege levels for allowing access to particular commands. You can use this feature to protect the system from unauthorized access.

There are 16 privilege levels - from level 15, which is the most restricted level (lowest privilege), to level 0, which is unrestricted (highest privilege).

A privilege is associated to each user and each command. Users can only execute commands with privilege levels that are equal to or less than (higher in nominal value) the privilege levels that are assigned to them.

Most of the commands have a privilege level 1. The common commands **exit, quit, yes, no, etc.** have privilege level 15, allowing all users to access them.

For example, users with privilege level 8 have access to all CLI commands with privilege levels from 8 to 15.

NOTE User privilege levels are not numbered consequently (i.e. 1-5) to ensure compatibility with the future versions of the device. Numbering shows the levels' priority only and is not used in the CLI.

The default privilege level assigned to users is level 0 (highest privilege).

NOTE Users' names, passwords and privileges are stored in the internal flash memory so they protected from interruptions in switch's power supply. For safety reasons, the passwords cannot be retrieved in any human-readable form.

Table 4-1 shows the CLI privilege levels.

Table 4-1 Command Privilege Levels

Privilege	Description
administrator	(0): Full read/write privilege without restriction. The access to the security settings (user/password management commands; debug commands; license management commands, software upgrade, reload and script FS) is allowed.
net-admin	(4): Read/write privilege without access to the security, debug and other administrative settings (user/password management commands; debug commands; license management commands, software upgrade, reload and script FS)
technician	(8): Read/write privilege for Layer2, Read-only privilege for Layer3
user	(12): Read-only privilege that allows access to all show commands; general commands: exit, quit, yes, no; show commands; enable, disable commands, ping and traceroute commands

Privilege	Description
guest	(15): Read-only privilege in non-privileged mode (cannot execute the enable command)

RADIUS Authentication and Privilege Groups

In addition to the RADIUS server configuration, the authentication and privilege groups require the following steps:

1. Copy an additional file, for example with name dictionary.nokia, to the same folder in which the RADIUS configuration files are installed.

2. For all user, assign a privilege in the users file (refer to the example in dictionary.nokia file).

3. Add the dictionary.nokia file to the dictionary file that is part of the RADIUS configuration files.

Dot1x users with assigned Administrator privilege have two user names and passwords - one required from the for dot1x configuration and one for authentication.

The following example describes how to assign privilege to users through RADIUS authentication. The example refers only to freeRADIUS server authentication. The format may be different for other distributions of RADIUS server.

In general privilege levels are vendor specific attributes and are between 0 and 15. Users without privilege or wrong privilege are assigned privilege "*Guest*".

1. To describe Nokia vendor specific extensions, add a file with the name dictionary.nokia to RADIUS dictionaries. The file dictionary.nokia contains the following text:

```
VENDOR                          NOKIA       738

ATTRIBUTE               NOKIA-privilege-group   1     integer   NOKIA

VALUE                   NOKIA-privilege-group   Administrators     0
VALUE                   NOKIA-privilege-group   Network-admins     4
VALUE           NOKIA-privilege-group    Technicians             8
VALUE                   NOKIA-privilege-group   Users             12
VALUE                   NOKIA-privilege-group   Guests            15
```

2. Include the file dictionary.nokia in the main dictionary file:

```
INCLUDE  /usr/local/etc/raddb/dictionary.nokia
```

3. Configure the users by typing in the file *users* the following:

```
 test                    Auth-Type := Local, User-Password == "test"
                         Reply-Message = "Hello, %u",
                         Nokia-privilege-group = Network-admins
```

Nokia-privilege-group is the vendor-specific extension that carries the privilege information.

Supported Standards, MIBs and RFCs

Standards

No Standards are supported by this feature.

MIBs

No MIBs are supported by this feature.

RFCs

No RFCs are supported by this feature.

Default User Privilege Levels Configuration

Table 4-2 shows the default user privilege levels configuration.

Table 4-2 User Privilege Level Default Configuration

Parameter	Default Value
User privilege level for local users	Administrator (0)
User privilege level for RADIUS users	Guest (15)

Configuring and Displaying User Privileges

Table 4-3 lists the user privilege configuration and display commands.

Table 4-3 User Privilege Commands

Command	Description
username	Establishes a username-based authentication system.
show privilege	Displays the privilege level that is assigned to the current user.

Creating a New User with a Privilege Level

The **username** command, in Global Configuration mode, establishes a username-based authentication system.

The command creates a new user, assigns a password to this user, and specifies the access privilege level for this user.

If a password confirmation is required, the second password must be identical to the first.

By default, the local user is assigned privilege level 0 and RADIUS users are assigned privilege level 15.

Command Syntax

```
device-name(config)#username USER-NAME password PASSWORD [CONFIRM-PASSWORD] [group {administrators|net-admins|technicians|users|guests}]
```

Argument Description

USER-NAME	Specifies the name of the user. A character string consisting of any characters except for blank spaces and question marks.
password PASSWORD	The password assigned to the user. A character string without blank spaces.
CONFIRM-PASSWORD	Type the password again for confirmation. Type the password again for confirmation.
group	Sets the privilege group for the user. If the **group** option is not used, the user will be assigned Administrators privilege.
administrators	Assigns the user group Administrators privilege, with full read/write privilege without restrictions.
net-admins	Assigns the user group Net-admins privilege, with read/write privilege without access to security settings, software upgrade, debug settings, reload and script File System.
technicians	Assigns the user group Technicians privilege, with read/write privilege for Layer 2 and read-only privilege for Layer 3.
users	Assigns the user group Users privilege, with read-only permission.
guests	Assigns the user group Guests privilege, with read-only privilege in non-privileged mode

Example

The following example shows how to create a user and assign a privilege level to this user:

```
device-name(config)#username ME password YES group users
```

Displaying the User's Privilege Level

The **show privilege** command, in Privileged (Enable) mode, displays the assigned user privilege level.

Command Syntax

```
device-name#show privilege
```

Example

```
device-name#show privilege
Current user privilege is ADMIN
```

Displaying Users

The **show users** command, in either View or Privileged (Enable) mode, lists the users configured on the device that have lower or same user privileges as the current user. This means that only users with Administrator privilege can see all other users.

Command Syntax

```
device-name#show users
```

Example

```
device-name#show users
how users
Local users:
------------
 Username: JohnSmith  Privilege: Administrator
 Username: AnnKay  Privilege: Guest
 Username: JoeBlack  Privilege: Network-Admin

Total users: 3
device-name #
```

5. Ethernet Interface Configuration

Introduction

The ESB26 switch supports simultaneous, parallel conversations between Ethernet segments. Switched connections between Ethernet segments last only for the duration of the packet. New connections can be made between different segments for the next packet.

The ESB26 solves congestion problems caused by high-bandwidth devices and a large number of users by assigning each device to its own 100 or 1000 Mbps segment.

Because the major bottleneck in Ethernet networks is usually due to collisions, an effective solution is full-duplex communication, an option for each port on the switches (note that Gigabit Ethernet ports also support half duplex). Normally, Ethernet operates in half-duplex mode, which means that stations can either receive or transmit. In full-duplex mode, two stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, the effective Ethernet bandwidth is 200 Mbps for Fast Ethernet ports and 2 Gbps for Gigabit Ethernet ports.

Switching Frames between Segments

Each Ethernet port on the switch can connect to a single workstation or server, or to a hub through which workstations or servers connect to the network.

When stations on different ports need to communicate, the switch forwards frames from one port to the other at wire-speed to ensure that each session receives the full available bandwidth.

To switch frames between ports efficiently, the switch maintains an address table. When a frame enters the switch, it associates the Media Access Control (MAC) address of the sending station with the port on which it was received.

Building the Address Table

The switch builds the address table by using the source address of the frames received. When the switch receives a frame for a destination address not yet listed in its address table, it floods the frame to all ports of the same virtual LAN (VLAN) except for the port that received the frame. When the destination station replies, the switch adds its relevant source address and port ID to the address table. The switch then forwards subsequent frames to a single port without flooding them to all ports.

The address table can store up to 16K address entries without flooding any entries. The switch uses an aging mechanism, defined by a configurable aging timer, so that if an address remains inactive for a specified number of seconds, it is removed from the address table.

Supported Standards, MIBs and RFCs

Standards

IEEE 802.3 Ethernet

IEEE 802.3u Fast Ethernet

IEEE 802.3x Flow Control

IEEE 802.3z Gigabit Ethernet

MIBs

RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets:MIB-II* (interface table)

RMON MIB

Private MIB, *batm_switch*.mib

RFCs

RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets:MIB-II*

Default Fast and Giga Ethernet Ports Configuration

Table 5-1 shows the default Fast Ethernet and Giga Ethernet Ports configuration.

Table 5-1 Fast Ethernet and Giga Ethernet Ports Default Configuration

Parameter	Default Value
Interface state	Enabled
Port name	None
Backpressure mode	Disabled
Duplex speed	For Giga Ethernet Fiber: Auto-negotiation For Fast Ethernet and Giga Ethernet Copper: Auto-negotiation
Flow Control mode	Disabled

Port's PVID	1
Remote fault detect	Disabled
Crossover detection	Automatic
Port management	Enable

Configuring and Displaying Fast and Giga Ethernet Ports

Interface Configuration Commands

Table 5-2 lists the Fast and Giga Ethernet Ports configuration commands.

Table 5-2 Fast and Giga Ethernet Configuration Commands

Command	Description
interface	Enables configuration of a specific physical interface.
shutdown	Disables the interface (to receive, forward and learn).
name	Assigns a name to the Fast Ethernet or Giga Ethernet port to facilitate switch administration.
duplex-speed	Specifies the port speed.
backpressure	Changes the backpressure mode.
flow control	Changes the flow control mode.
default vlan	Changes the default VLAN (PVID) of the configured interface.
remote-fault-detect	Enables remote fault detection on the configured interface that is connected to a 100Base Fiber pair. (Not relevant for ESB26.)
crossover	Enables crossover detection which allows the switch port to automatically detect transmit and receive of the Ethernet cable (i.e., the type of the cable is irrelevant).

Accessing the Interface Configuration Mode

The **interface** command, in Global Configuration mode or Interface Configuration mode, enables configuration of a specific physical interface.

The command changes the switch's configuration mode into Interface Configuration mode. Following execution of the command, the prompt line displays the interface *unit*, *slot* and *port* numbers. If you apply this command when the switch is in Interface Configuration mode, the mode is changed to the specified Interface Configuration mode (for example, you can use this command to change the mode from Interface 1/1/1 Configuration mode to Interface 1/1/2 Configuration mode).

When the switch enters interface-configuration mode, this is indicated by changing the command prompt - it displays the interface unit and the slot and port numbers.

Command Syntax

```
device-name(config)#interface UU/SS/PP|range|agXX
device-name(config-if UU/SS/PP)#

device-name(config-if UU1/SS1/PP1)#interface UU2/SS2/PP2|range|agXX
device-name(config-if UU2/SS2/PP2)#
```

Argument Description

UU/SS/PP	Represent the unit, slot and port numbers of the configured interface.
range	Configures a group of interfaces at a time. Individual interfaces are separated by commas, range is indicated with hyphen, e.g. 1/1/1, 1/1/2-1/1/6. Entering Interface Group Configuration mode is indicated by the command prompt changing to `(config-if-group)#`.
agXX	Link aggregation interface's name (e.g. ag01).

Example 1

Accessing Interface Configuration mode for interface 1/1/2

```
device-name(config)#interface 1/1/2
device-name(config-if 1/1/2)#
device-name(config)#
```

Example 2

Specifying a range of interfaces and changing the Spanning Tree path cost for them:

```
device-name(config)#interface range 1/1/4-1/1/6
device-name(config-if-group)#spanning-tree path-cost 200
device-name(config-if-group)#
```

Disabling an Interface

The **shutdown** command, in Interface Configuration mode, disables the interface (to receive, forward and learn). The **no** form of this command enables the interface.

The **shutdown** command disables all functions on the specified interface. This command also marks the interface as unavailable. To check whether an interface is disabled, use the **show interface** command in Privileged (Enable) mode. An interface that has been shut down is shown as administratively down in the display issued by the **show interface** command.

By default, the interface is enabled (active).

Command Syntax

```
device-name(config-if UU/SS/PP)#shutdown
device-name(config-if UU/SS/PP)#no shutdown
```

Setting a Name to the Fast Ethernet or Giga Ethernet Port

The **name** command, in Interface Configuration mode, assigns a name to the Fast Ethernet or Giga Ethernet port to facilitate switch administration. The **no** form of the command removes the port name.

By default, the port has no name.

Command Syntax

```
device-name(config-if UU/SS/PP)#name NAME
device-name(config-if UU/SS/PP)#no name
```

Argument Description

NAME	String of up to 16 characters which represents the port name. Spaces are not allowed.

Setting Duplex Speed

The **duplex-speed** command, in Interface Configuration mode, specifies the port speed. You can set the port duplex mode to full or half duplex for Fast Ethernet and Ethernet ports.

The Giga copper ports have *crossover detection*. The crossover detection allows the switch port to automatically detect transmit and receive polarity of the Ethernet cable (e.g. the type of the cable is irrelevant).

By default, the switch is configured to use auto-negotiation to determine the port speed and duplex setting for each port, except for the Fast Ethernet Fiber ports that are set to Full-100. You can manually configure the duplex setting and the speed of 10/100/1000 Mbps ports.

Command Syntax

```
device-name(config-if UU/SS/PP)#duplex-speed VALUE
```

Argument Description

VALUE	The interface's duplex speed type, restricted to the set of literal values listed in Table 5-3.

Table 5-3 Duplex Speed Argument Values

Value	Description
autonegotiate	When this option is selected, the port automatically finds the highest speed that can be supported on the link.
half-10	Half duplex at 10Mbps
full-10	Full duplex at 10Mbps
half-100	Half duplex at 100Mbps
full-100	Full duplex at 100Mbps
half-1000	Half duplex at 1Gbps
full-1000	Full duplex at 1Gbps

Setting the Backpressure Mode

The **backpressure** command, in Interface Configuration mode, changes the backpressure mode. Backpressure is a technique for ensuring that a transmitting port does not send too much data to a receiving port at a given time. When the buffer capacity of a receiving port is exceeded, it sends a *Jam message* to the transmitting port to halt transmission.

Backpressure is available only if the port transmits or receives at Half Duplex speed.

By default, backpressure is disabled.

NOTE Backpressure is available only if the port transmits or receives at Half Duplex speed.

Command Syntax

```
device-name(config-if UU/SS/PP)#backpressure {enable | disable}
```

Argument Description

enable	Enables backpressure on the configured interface.
disable	Disables backpressure on the configured interface

Setting the Flow Control Mode

The **flow control** command, in Interface Configuration mode, changes the flow control mode. Flow control is a technique for ensuring that a transmitting port does not send too much data to a receiving port at a given time.

If a buffer on a port runs out of space, the port transmits a special packet that requests remote ports to delay sending packets for a period of time. The **flow control** command is available only if the port transmits or receives in Full Duplex.

By default the flow control is disabled.

NOTE The flow control command is available only if the port transmits or receives in Full Duplex.

Command Syntax

```
device-name(config-if UU/SS/PP)#flow control {enable | disable}
```

Argument Description

enable	Enables flow control on the configured interface.
disable	Disables flow control on the configured interface.

Setting the Port PVID

The **default vlan** command, in Interface Configuration mode, changes the default VLAN (PVID) of the configured interface. The **no** form of this command changes the default VLAN of the interface to VLAN 1.

To view the default VLAN configuration, use the **show interface** command or **show interface *UU/SS/PP*** command in Privileged (Enable) or Interface Configuration mode.

The PVID of the interface can also be set by the **add ports default** command in Specific VLAN Configuration mode. For more information regarding the VLAN commands see "*Commands to Configure VLAN Settings*".

By default, the PVID is VLAN 1.

NOTE You can also change the default VLAN of an interface by using the add ports default command in Specific VLAN Configuration mode.

Command Syntax

```
device-name(config-if UU/SS/PP)#default vlan <vlan-id>
device-name(config-if UU/SS/PP)#no default vlan
```

Argument Description

vlan-id	The default VLAN (PVID) for the specified interface. The range is <1-4094>. By default, the default VLAN (PVID) for all the interfaces is 1.

Setting Remote Fault Detection

The **remote-fault-detect** command, in Interface Configuration mode, enables remote fault detection on the configured interface that is connected to a 100Base Fiber pair. The **no** form of this command disables the remote fault detection.

When remote fault detection is enabled on such an interface, the switch indicates link down on the port if the remote peer detects link down.

NOTE The remote-fault-detect command is available only on 100Base Fiber ports. (Not relevant for ESB26.)

Command Syntax

```
device-name(config-if UU/SS/PP)#remote-fault-detect
device-name(config-if UU/SS/PP)#no remote-fault-detect
```

Setting Crossover Detection

The **crossover** command, in Interface Configuration mode, enables crossover detection which allows the switch port to automatically detect transmit and receive of the Ethernet cable (i.e., the type of the cable is irrelevant). The **no** form of this command sets the crossover detection to automatic mode.

To view the crossover detection status, use the **show interface** command in Privileged (Enable) mode.

MDI/MDIX is a type of Ethernet port connection according to the IEEE 802.3 standard using twisted pair cabling. Network adapter cards on computers and workstations generally connect to the network via RJ-45 interface ports that use pins 1 and 2 for transmit and 3 and 6 for receive. Uplink ports on hubs and switches use the same pin assignments. Such ports are called Medium Dependent Interface (MDI) ports. Normal ports on hubs and switches use the opposite pin assignment, i.e. – pins 1 and 2 are used for receive and pins 3 and 6 are used for transmit. Such ports are called MDIX (MDI-crossed) ports.

In order to feed the transmitted data from one end of the connection to the receive pins on the other end:

MDI (computers and uplink) ports are connected to MDIX (hub or switch) ports via straight-through twisted pairs.

MDIX (normal) ports on switches or hubs are connected to each other via a crossover cable.

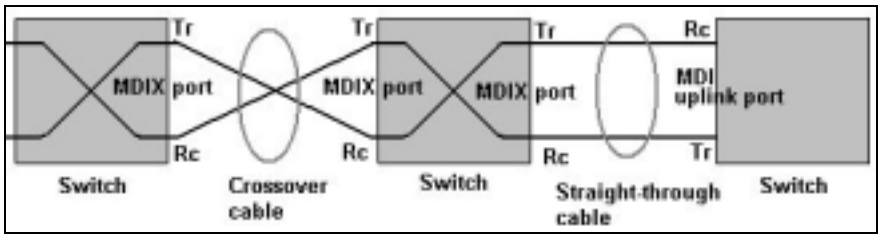


Figure 5-1 Crossover and Straight-Through Connections

When automatic crossover detection is defined, you can interconnect any combination of MDI/MDIX ports using either type of cable (crossover or straight-through) without distinction.

By default, crossover detection is automatic.

Command Syntax

```
device-name(config-if UU/SS/PP)#crossover {auto | mdi | mdix}
device-name(config-if UU/SS/PP)#no crossover
```

Argument Description

auto	Sets automatic crossover detection on the port.
mdi	Sets the manually port to MDI (Medium Dependent Interface).
mdix	Sets the manually port to MDIX (MDI crossover).

Displaying the Interface Settings and Statistics

Table 5-4 lists the Fast Ethernet and Giga Ethernet Ports displaying commands.

Table 5-4 Fast Ethernet and Giga Ethernet Displaying Commands

Command	Description
show interface	Displays the settings of the physical interfaces.
show interface statistics	Displays the interface statistics and packet counters.

Displaying the Interface Configuration Settings

The **show interface** command, in Privileged (Enable) or Interface Configuration mode, displays the settings of the physical interfaces. If the interface argument is specified, the command will display the configuration of the specified interface.

Command Syntax

```
device-name#show interface [UU/SS/PP]
```

Argument Description

UU/SS/PP	(Optional). Represent the Unit, Slot and Port numbers respectively, each in one or two decimal digits.

Example 1

The following example displays the settings of all the switch's interfaces:

```
device-name#show interface
=================================================================
|port |name |type |state|link|duplspeed |flow |backpres|default vlan
+-----+-----+-----+-----+------------+-----+--------+------------
1/1/1        eth   enable  down unknown   disable disable   0003
1/1/2        eth   enable  down unknown   disable disable   0001
1/1/3        eth   enable  down unknown   disable disable   0001
1/1/4        eth   enable  down unknown   disable disable   0001
1/1/5        eth   enable  down unknown   disable disable   0001
1/1/6        eth   enable  down unknown   disable disable   0001
1/1/7        eth   enable  down unknown   disable disable   0001
1/1/8        eth   enable  down unknown   disable disable   0001
```

Example 2

The following example displays the settings of a specific interface:

```
device-name#show interface 1/1/8
Name                 =
Type                 = 100BaseTX (L3)
EnableState          = enable
Link                 = up
Duplex speed mode    = autonegotiate
Duplex speed status  = full-100
Flow control mode    = disable
Flow control status  = disable
Backpressure         = disable
Broadcast limit      = unlimited
Default VLAN         = 1
Port Crossover       = AUTO MDI/MDIX
```

Displaying the Interface Statistics

The **show interface statistics** command, in Privileged (Enable) mode, displays the interface statistics and packet counters. Table 5-5 describes the counters displayed by the **show interface statistics** command and Table 5-6 describes the counters displayed by the **show interface statistics extended** command.

NOTE The MaxFrameSize refers to the maximum supported packet size depending on the configuration (1518 bytes or 6 Kbytes).

Command Syntax

```
device-name#show interface [UU/SS/PP] statistics [extended]
```

Argument Description

UU/SS/PP	(Optional) Interface unit, slot and port number.
extended	(Optional). Displays additional packet counters.

Example 1

The following example uses the **show interface statistics** command for a specified interface to display various packet counters:

```
device-name#show interface 1/1/1 statistics
Octets                0        In/OutPkts 64                        0
Collisions            0        In/OutPkts 65-127                    0
Broadcast             0        In/OutPkts 128-255                   0
Multicast             0        In/OutPkts 256-511                   0
CRCAlignErrors        0        In/OutPkts 512-1023                  0
Undersize             0        In/OutPkts 1024-MaxFrameSize         0
Oversize              0        TotalInPkts                          0
Fragments             0        TotalIn/OutPkts                      0
Jabbers               0        Last5secInPkts                       0
DropEvents            0        Last1minInPkts                       0
Down count            0        Last5minInPkts                       0
```

Table 5-5 Counters Displayed by the Show Interface Statistics Command

Counter	Description
Octets	This counter is incremented once for every data octet of all received packets. This includes data octets of rejected and local packets that are not forwarded to the switching core for transmission. This counter should reflect all the data octets received on the line. For oversized packets, when they exceed the allocated buffer-size, only buffer-size bytes are counted and all the rest of the bytes are not.
Collisions	This counter is incremented once for every received packet when a Collision Event has been detected.
Broadcast	This counter is incremented once for every good Broadcast packet received.
Multicast	This counter is incremented once for every good Multicast packet received.
CRCalignErrors	This counter is incremented once for every received packet that meets all the following conditions: Packet data length is between 64 and MaxFrameSize bytes inclusive. Packet has invalid CRC (non-A also counted packets with an odd number of nibbles). Collision Event has not been detected. Late Collision Event has not been detected.
Undersize	This counter is incremented once for every received packet that meets all the following conditions: Packet data length is less than 64 bytes. Collision Event has not been detected. Late Collision Event has not been detected. Packet has valid CRC.

Counter	Description
Oversize	This counter is incremented once for every received packet that meets all the following conditions: Packet data length is greater than MaxFrameSize. Packet has valid CRC.
Fragments	This counter is incremented once for every received packet that meets all the following conditions: The packet's data length is less than 64 bytes, or the packet is without SFD (Start Frame Delimiter) and is less than 64 bytes in length. Collision Event has not been detected. Late Collision Event has not been detected. Packet has invalid CRC.
DropEvents	Not supported.
Jabbers	This counter is incremented once for every received packet that meets all the following conditions: Packet data length is greater than MAXFRAME-SIZE. Packet has invalid CRC.
TotalInPkts	This counter is incremented once for every received packet. This includes rejected and local packets that are not forwarded to the switching core for transmission. This counter should reflect all packets received on the line.
In/OutPkts 64	This counter is incremented once for every received and transmitted packet that is 64 bytes in size. This counter includes rejected, received, and transmitted packets.
In/OutPkts 65-127	This counter is incremented once for every received and transmitted packet that is 65 to 127 bytes in size. This counter includes rejected, received, and transmitted packets.
In/OutPkts 128-255	This counter is incremented once for every received and transmitted packet that is 128 to 255 bytes in size. This counter includes rejected, received, and transmitted packets.
In/OutPkts 256-511	This counter is incremented once for every received and transmitted packet that is 256 to 511 bytes in size. This counter includes rejected, received, and transmitted packets.
In/OutPkts 512-1023	This counter is incremented once for every received and transmitted packet that is 512 to 1023 bytes in size. This counter includes rejected, received, and transmitted packets.
In/OutPkts 1024-1518	This counter is incremented once for every received and transmitted packet that is 1024 to MaxFrameSize bytes (1518) in size. This counter includes rejected, received, and transmitted packets.
TotalIn/OutPkts	This counter is incremented once for every received and transmitted packet that is 64 to MaxFrameSize bytes in size. This counter includes rejected, received, and transmitted packets.

Counter	Description
Down Count	This counter is incremented once for every disconnection of the port. The counter is initialized in any of the following cases: When the switch starts running (provided that the link to the port is connected), the counter is initialized to zero. When the module is inserted at run-time (hot-swapped), the counter is initialized to one. If the link to the port is connected for the first time during run-time, the counter is initialized to one.

Example 2

The following example uses the **extended** keyword to display additional packet counters:

```
device-name#show interface 1/1/1 statistics extended
InOctets          41061272        OutOctets           7948538
InUcastPkts          73572        OutUcastPkts          73825
InNUcastPkts          3873        OutNUcastPkts         28439
InDiscards               0        OutDiscards               N/A
InErrors                 1        OutErrors                 N/A
InUnknownProtos        N/A
```

Table 5-6 Counters Displayed by the Show Interface Statistics Extended Command

Counter	Description
InOctets	This counter is incremented once for every data octet of all received packets. This includes data octets of rejected and local packets that are not forwarded to the switching core for transmission. This counter should reflect all the data octets received on the line. For oversized packets, the exceeded allocated buffer-size, only buffer-size bytes are counted and all the rest of the bytes are not.
InUcastPkts	This counter is incremented once for every good unicast packet (not including Multicast and Broadcast packets) received.
InNUcastPkts	This counter is incremented once for every good Broadcast and Multicast packet received.
InDiscards	This counter is incremented once for every incoming packet dropped due to lack of receive buffers or overload on the address recognition machine.
InErrors	This counter is incremented once for every bad received packet. This includes rejected and local packets that are not forwarded to the switching core for transmission. It counts the difference between the total received packets and the total received good packets (Unicast, Multicast and Broadcast).
InUnknownProtos	Not supported.
OutOctets	This counter is incremented once for every data octet of a transmitted good packet.
OutUcastPkts	This counter is incremented once for every transmitted good Unicast packet (not include Multicast and Broadcast packets).
OutNUcastPkts	This counter is incremented once for every transmitted good Broadcast and Multicast packet.

Counter	Description
OutDiscards	Not supported.
OutErrors	Not supported.

Clearing the Interface Statistics

Table 5-7 lists the Fast Ethernet and Giga Ethernet interfaces commands for clearing the interfaces statistics.

Table 5-7 Interface Clearing Statistics Commands

Command	Description
reset	Clears the statistics of the configured port.
clear interface statistics	Clears the statistics of all the ports.

Clearing the Port Statistics

The **reset** command, in Interface Configuration mode, clears the statistics of the configured port. If you specify the keyword **all**, the command clears the statistics of all the ports.

Command Syntax

```
device-name(config-if UU/SS/PP)#reset [all]
```

Argument Description

all	(Optional). Clears the statistics of all the ports.

Clearing All Ports Statistics

The **clear interface statistics** command, in Privileged (Enable) mode, clears the statistics of all the ports.

Command Syntax

```
device-name#clear interface statistics
```

Configuring and Displaying Management Ports

Table 5-8 lists the commands for configuring and displaying switch-management on ports.

Table 5-8 VLAN Switch-Management Commands

Command	Description
port management	Controls access to switch management on specified ports.

show port management	Displays which ports provide management access.

Setting Management Ports

The **port management** command, in Global Configuration mode, controls access to/from switch management on specified ports. The **no** form of this command blocks access to the switch's management on specified ports for both outgoing and incoming management packets.

Use the **port management** command to restrict switch management access to a list of ports that you specify.

Before applying the **port management** command, verify that the following condition is met:

You must be able to move your network management station to a switch port assigned to the same port as the management port.

If port management is disabled, the following will be disallowed:

- Telnet to the switch
- SSH to the switch
- SNMP management
- SNMP traps and informs
- Ping to the switch
- TFTP download or upload
- Outgoing Syslog messages

By default, management of the switch is accessible through all ports. Also, all outgoing management packets are with highest priority (7) when port is tagged.

NOTE 

You can also disable management on a VLAN by the management command in VLAN Configuration mode. Management traffic on a VLAN is allowed on a port that is a member of that VLAN only if management is enabled both on the port and on the VLAN.

Command Syntax

```
device-name(config)#port management PORT-LIST
device-name(config)#no port management PORT-LIST
```

Argument Description

PORT-LIST	List of ports, specified by the following options: UU/SS/PP – (unit, slot and port number, e.g. – 1/1/8) specifying a single port; UU – (1 or 2-digit unit number) specifying all ports on unit; UU/SS – (unit and slot number) specifying all ports on slot; A hyphenated range of ports, e.g. - 1/1/9-1/1/16 or 1/2-1/3; Several port numbers and/or ranges, separated by commas, e.g. – 1/1, 1/2/3-1/2/6, 1/2/8.

Displaying the Management Ports

The **show port management** command, in Privileged (Enable) mode, displays which ports provide management access.

Command Syntax

```
device-name#show port management
```

Example

```
device-name#show port management
Management ports: 1/1/2,1/1/5
```

Related Commands

Table 5-9 shows the commands related to Fast and Giga Ethernet port configuration.

Table 5-9 Fast and Giga Ethernet Port Configuration Related Commands

Command	Description	Described in
add ports default	Sets PVID of specified port(s).	Commands to Configure VLAN Settings, **add ports default**
management	Controls access to switch management on specified VLANs.	Commands to Configure VLAN Settings, **management**

6. Port Security

Introduction

You can use port security to block input to a port when the MAC address of the station attempting to access the port does not match any of the MAC addresses specified for that port. Alternatively, you can use port security to filter traffic destined to or received from a specific host based on the host MAC address.

After establishing the maximum number of MAC addresses on a port, the secure MAC addresses can be configured manually or learned dynamically. You can manually configure all the secure MAC address or only some of them.

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or dynamically learned on the port. If a MAC address of a device attached to the port differs from the list of secure addresses, the port either shuts down permanently or drops incoming packets from the insecure host and sends trap message to the Simple Network Management Protocol (SNMP) manager. The port's behavior depends on the configuration that determines its response to a security violation.

Configuring and Displaying Port Security Settings

Table 6-1 Port Security Commands

Command	Description
port security	Enables port security on the configured interface.
show port security	Displays the port security configuration.

Description of Commands

port security

The **port security** command, in Interface Configuration mode, enables port security on a port and restricts the use of the port to a user-defined group of stations. The **no** form of this command returns the port to its default value.

If the **port security** option is activated on a port, only **SECURED** MAC addresses that are configured to this port are permitted to connect to this port. A station with a MAC address that has not been configured appropriately in the MAC address table will produce an **address violation** event. See How Entries are added to the FDB.

If no action is defined, the default action is **trap**. If no maximum number is defined for secure addresses support, all the addresses will be learned as secured.

Command Syntax

```
device-name(config-if UU/SS/PP)#port security [action {shutdown| trap}|max-
mac-count <number-of-addresses>]
device-name(config-if UU/SS/PP)#no port security [action {shutdown| trap}]
```

Argument Description

action shutdown	Disable the port when a security violation occurs.
action trap	Generate an SNMP trap when a security violation occurs. The MAC address that will pass the maximum allowed will be learned as filtered.
max-mac-count <number-of-addresses>	The maximum numbers of secure addresses that this port can support. The range is <1 – 256>.

NOTES

1. In each port security command, the arguments are optional and mutually exclusive. However, you can specify an action (shutdown or trap) in one port security command and specify the maximum number of secure addresses (max-mac-count) in a second port security command for the same port. Both settings will be effective.
2. By default, port security is disabled. When port security is enabled, the default action is to generate an SNMP trap.

show port security

The **show port security** command, in Privileged (Enable) mode, displays the security status of the specified port, as configured by the **port security** command described below. If the argument is not specified, the security status of all ports configured with the command is displayed.

A port can be either **secured**, meaning that only secured MAC-addresses can be attached to it, or **not secured**.

Command Syntax

```
device-name#show port security [UU/SS/PP]
```

Argument Description

UU/SS/PP	Unit, Slot and Port numbers respectively of the secured port, each in one or two decimal digits.

Examples

1. The following example configures various port security settings for ports 1/1/2, 1/1/3, 1/1/4 and 1/1/8:

```
device-name(config)#interface 1/1/2
device-name(config-if 1/1/2)#port security
device-name(config-if 1/1/2)#interface 1/1/3
device-name(config-if 1/1/3)#port security action shutdown
device-name(config-if 1/1/3)#interface 1/1/4
device-name(config-if 1/1/4)#port security max-mac-count 6
```

```
device-name(config-if 1/1/4)#interface 1/1/4
device-name(config-if 1/1/8)#port security action shutdown
device-name(config-if 1/1/8)#port security max-mac-count 10
```

The configured settings are displayed by the **show** command in Privileged mode as follows:

```
device-name#show port security

|port num    |action      |max-mac-count   |current mac-count|
|------------+------------+----------------+-----------------|
|1/1/2       |trap        |not-limited     |0                |
|1/1/3       |shutdown    |not-limited     |0                |
|1/1/4       |trap        |6               |0                |
|1/1/8       |shutdown    |10              |0                |
```

2. The following example sets the maximum number of addresses to 3. The system is allowed to learn up to 3 MAC addresses and to send SNMP traps on in the event of over-learning.

   - First, configure the SNMP trap host to receive traps (See the SNMP Server Configuration chapter).

```
device-name(config)#snmp-server group Gr v1 read none write none notify
viewAll_XXX
device-name(config)#snmp-server user public group Gr v1
device-name(config)#snmp-server notify NOTIFY-NAME tag1
device-name(config)# snmp-server target-param MyParam public v1
device-name(config)#snmp-server target-addr MyHost 9.0.0.0 162 MyParam tag1
```

NOTE

The snmp-server notify command is repeated for each trap type (Refer to the Configuring and Displaying the SNMP Server Settings section for details.). The trap type is represented by the NOTIFY-NAME character string and a tag (that has the same name as the notify name).

   - Next, configure the port to learn a maximum of 3 MAC addresses.

```
device-name(config)#interface 1/1/2
device-name(config-if 1/1/2)#port security max-mac-count 3
```

   - Now, return to Config mode and define 3 MAC addresses to be learned:

```
device-name(config)#mac-address-table secure 00:02:4b:82:60:e2 interface 1/1/2 vlan 2
device-name(config)#mac-address-table secure 00:02:55:58:0d:8c interface 1/1/2 vlan 2
device-name(config)#mac-address-table secure 00:02:55:98:52:f4 interface 1/1/2 vlan 2
```

   - In Privileged mode, check that the MAC addresses were learned.

```
device-name#show mac-address-table
```

The screen should display the settings for interface 1/1/2 as follows:

```
+==========+====================+=========+===========+==========
|   vid    |  mac               |  port   |  status   | priority
+----------+--------------------+---------+-----------+----------
|   0000   |  00:a0:12:07:13:29|  0/0/0  |  self     | 0
|   0001   |  00:a0:12:07:13:29|  0/0/0  |  self     | 0
|   0002   |  00:02:4b:82:60:e2|  1/1/2  |  secure   | 0
|   0002   |  00:02:55:58:0d:8c|  1/1/2  |  secure   | 0
```

```
|   0002    |  00:02:55:38:52:f4|  1/1/2  |  secure   | 0
|   0002    |  00:40:95:30:0b:f8|  1/1/3  |  dynamic  | 0
```

- Finally, check the port security definitions:

```
device-name#show port security 1/1/2
```

Depending on previous settings, the screen should display results as follows:

```
The port is : secured
Action on security violation :send a trap
Max secured addresses : 3
Current secured addresses : 3
```

7. Link Aggregation Groups (LAGs)

Introduction

Link Aggregation Groups (LAGs), also known as trunks, provide increased bandwidth and high reliability while saving the cost of upgrading the hardware. By combining several interfaces into one logical link, LAGs offer network channels tailored to need, filling the gaps between 10 Mbps, 100 Mbps and 1 Gbps with intermediate bandwidth values. LAGs also enable bandwidths beyond the 100 Mb limit by aggregating multiple Mega ports (see the example in Figure 7-1).

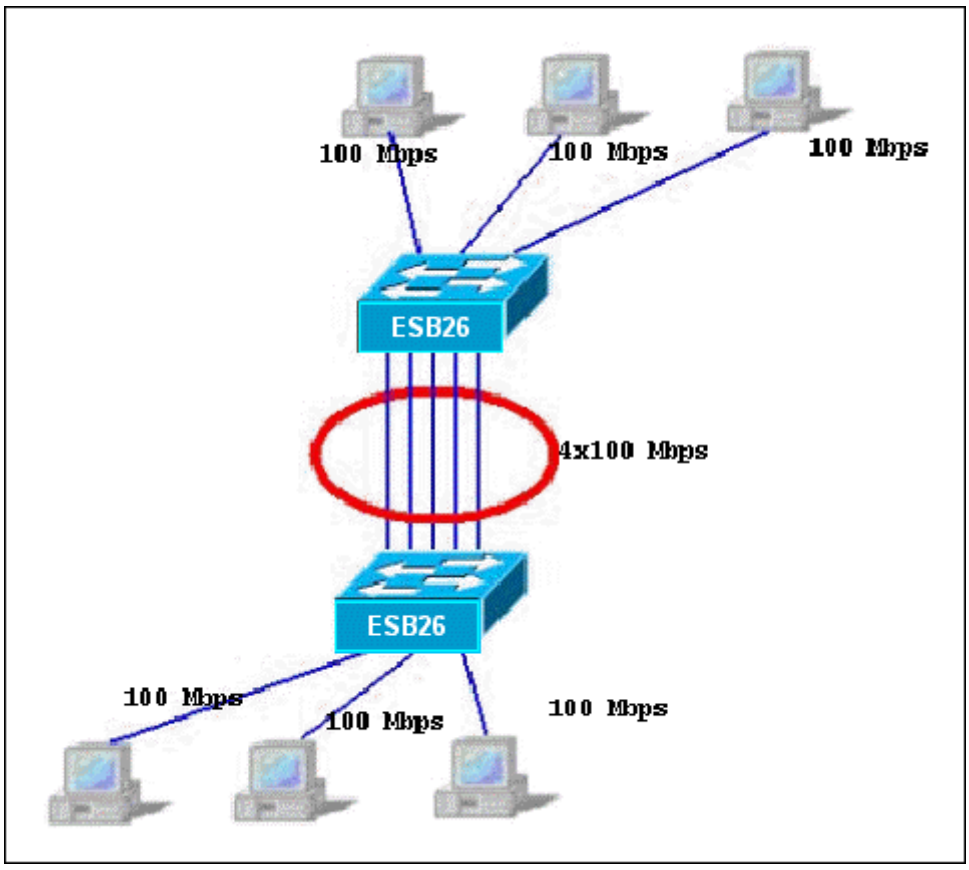


Figure 7-1: Four Ports Combined into a Link Aggregation Group

The Link Aggregation Control Protocol (LACP) ensures smooth and steady traffic flow by automating the configuration, re-configuration and maintenance of aggregated links. The LACP feature dynamically adapts aggregated links to changes in traffic conditions. Load sharing is maintained and automatically readjusted if a failure or recovery from failure occurs in any of the links that participate in a dynamic LAG.

BiNOS supports both static and dynamic LAGs. Static and dynamic LAGs can exist simultaneously on the same switch.

Feature Overview

Static Link Aggregation Groups (LAGs)

Static LAGs provide the ability to treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between two network devices. A static LAG balances the traffic load across the links in the channel. If a physical link within the static LAG fails, traffic previously carried over the failed link is moved to the remaining links. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group.

A static LAG consists of individual Fast Ethernet links bundled into a single logical link as shown in Figure 7-1: "Four Ports Combined into a Link Aggregation Group".

Benefits

Static LAGs provide the following benefits:

- **Increased bandwidth**

  The capacity of multiple interfaces is combined into one logical link. Besides increasing bandwidth, link aggregation also provides intermediate data rate levels between the standard data rates of 10 Mbps, 100 Mbps, and 1000 Mbps, as well as rates beyond 1000 Mbps if required.

- **Increased availability**

  If a link within a LAG fails or is replaced, the traffic is not disrupted and communication is maintained (even though the available capacity is reduced).

- **Load sharing**

  Traffic is distributed across multiple links, minimizing the probability that a single link be overwhelmed.

- **Use of existing hardware**

  Software replaces the need to upgrade the hardware to higher bandwidth capacity.

The Link Aggregation Control Protocol (LACP)

LACP, specified in the IEEE standard 802.3ad, provides a standardized means for dynamically exchanging information between two switches in order to configure and maintain link aggregation groups automatically. LACP can automatically detect the presence of other aggregation-capable network devices in the system. It enables you to determine which links in a system can be aggregated. For each aggregatable link, the switches exchange LACP frames in order to allocate the link to a Link Aggregation Group.

LACP Modes

The LACP interface supports two modes of operation, as follows:

Passive: The switch does not initiate the LAG, but understands the LACP packet. The switch will reply to the received LACP packet to eventually form the LAG if the other end (in *active* state) requests it to do so.

Active: The switch is willing to form an aggregate link, and initiate the negotiation. The link aggregate will be formed if the other end is running in LACP *active* or *passive* mode.

LACP Parameters

The following parameters are used in configuring LACP:

- ***System priority*** - Each switch running LACP must have a system priority. The system priority can be specified automatically or through the **link-aggregation lacp system-priority** command in Protocol Configuration mode. The switch uses the MAC address and the system priority to form the system ID that is also used during negotiation with other systems.
- ***Port priority*** - Each port in the switch must have a port priority. The port priority can be specified automatically or through the **link-aggregation lacp** command in Interface configuration mode. The port priority and the port number form the port identifier. The switch uses the port priority to decide which ports to put in standby mode when a hardware limitation prevents all compatible ports from aggregating.

When enabled, LACP always tries to configure the maximum number of compatible ports in a LAG, up to the maximum allowed by the hardware. If LACP is unable to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the LAG are put in hot standby state and are used only if one of the channeled ports fails.

Benefits

The goals and objectives of link aggregation are specified in the IEEE standard 802.3ad. Among these, LACP provides:

- **Rapid automatic configuration and reconfiguration**

  If physical connections are changed or fail, LACP automatically reconfigures the connection, typically within a second or less.

- **Deterministic behavior**

  The resulting aggregation can be determined by the capabilities of the individual links and their physical connectivity, regardless of the order in which events occur.

- **Low risk of duplication or misorder**

  There is a high probability that the order of frames is maintained and that frames are not duplicated, both in regular operation and during link reconfiguration.

LAG ID Numbers

LAG ID numbers are used to identify specific LAGs in configuration commands. LAG ID numbers uniquely identify the group of ports that participate in the LAG. You can define up to 7 LAGs. The valid LAG ID numbers are 1÷7.

MAC Addresses Learned on LAG Ports

You can see in the MAC address table the physical ports and the LAGs on which the MAC addresses were learned.

Each MAC address is shown with the number of the port on which it was physically learned and the name of the LAG group to which the port belongs.

For example, the LAG with the name AG07 comprises ports 1/1/1-1/1/5:

```
device-name#show mac-address-table
===+======+====================+==============+==========+==========+
 #  | VID  | Mac                | PORT         | STATUS   | PRIORITY |
---+------+--------------------+--------------+----------+----------+
 1 | 0001 | 00:00:00:01:12:03  | 1/1/3  AG07  |  dynamic | 0        |
 2 | 0001 | 00:00:00:01:12:04  | 1/1/4  AG07  |  dynamic | 0        |
 3 | 0001 | 00:00:00:01:12:05  | 1/1/5  AG07  |  dynamic | 0        |
 4 | 0001 | 00:00:00:01:12:06  | 1/1/1  AG07  |  dynamic | 0        |
 5 | 0001 | 00:00:00:01:12:07  | 1/1/2  AG07  |  dynamic | 0        |
 6 | 0001 | 00:00:00:01:12:08  | 1/1/3  AG07  |  dynamic | 0        |
 7 | 0001 | 00:00:00:01:12:09  | 1/1/4  AG07  |  dynamic | 0        |
 8 | 0001 | 00:00:00:01:12:0a  | 1/1/5  AG07  |  dynamic | 0        |
 9 | 0001 | 00:00:00:01:12:0b  | 1/1/1  AG07  |  dynamic | 0        |
10 | 0001 | 00:00:00:01:12:0d  | 1/1/1  AG07  |  dynamic | 0        |
11 | 0001 | 00:00:00:01:12:28  | 1/1/2  AG07  |  dynamic | 0        |
12 | 0001 | 00:00:00:01:12:29  | 1/1/3  AG07  |  dynamic | 0        |
13 | 0001 | 00:00:00:01:12:2a  | 1/1/2  AG07  |  dynamic | 0        |
14 | 0001 | 00:00:01:00:08:03  | 1/1/2  AG07  |  dynamic | 0        |
15 | 0001 | 00:00:01:00:12:03  | 1/1/12       |  dynamic | 0        |
16 | 0001 | 00:a0:12:11:29:82  |              |  self    |          |
```

Supported Standards, MIBs and RFCs

Standards

IEEE 802.3ad

MIBs

Private MIB, nokia_Ports_Aggregation.mib

RFCs

No RFCs are supported by this feature.

Prerequisites

The following guidelines apply to LAG configuration:

- You do not need to do any changes to existing higher-layer protocols or applications in order to use Link Aggregation.
- Links that cannot take part in Link Aggregation - due to their inherent capabilities or the capabilities of the devices to which they attach, or due to management configuration -operate as normal, individual links.
- LACP supports only point-to-point full-duplex links. Aggregations among more than two devices (multipoint aggregations) and half-duplex operation are not supported.
- All links in a Link Aggregation Group operate at the same data rate (e.g., 10 Mbps, 100 Mbps, or 1000 Mbps).
- The ports that participate in a LAG must all be of the same bandwidth. 10/100 BaseTx copper ports must belong to the same slot or device, but need not be contiguous (e.g. – you may include ports 1/1/3 and 1/1/5 in a LAG without including port 1/1/2).
- When the switch is connected to a LAN and Spanning Tree protocol is not active, physically connect the aggregated ports ONLY after LAG configuration is completed.

Default Link Aggregation Configuration

Table 7-1 shows the default Link Aggregation configuration.

Table 7-1 Link Aggregation Default Configuration

Parameter	Default Value
Static Link Aggregation	Disabled
Global Link Aggregation Control Protocol (LACP)	Disabled
Per port Link Aggregation Control Protocol (LACP)	Disabled
LACP system priority	32768

Parameter	Default Value
LACP port mode	Active
LACP port priority	32768

Configuring and Displaying LAGs

Configuring Static LAGs

To set the static LAG, set the ports participating in the static LAG. See Adding a Port to a Static Link Aggregation Group.

Table 7-2 lists the static LAG configuration commands.

Table 7-2 Static LAG Configuration Commands

Command	Description
link-aggregation static id	Sets a user-defined name for a specified static aggregate specified by the LAG id number.

Adding a Port to a Static Link Aggregation Group

The **link-aggregation static id** command, in Interface Configuration mode, adds the configured interface to the specified static link aggregation group. The **no** form of the command removes the configured interface from the static LAG to which it belongs.

By default, static LAG is disabled.

NOTE The link-aggregation static command replaces the trunk command.

Command Syntax

```
device-name(config-if UU/SS/PP)#link-aggregation static id <id-number>
device-name(config-if UU/SS/PP)#no link-aggregation
```

Configuring LACP

To set the LACP, proceed as follows:

1. Enable LACP on the switch. See Enabling/Disabling LACP Globally.

2. You can change the LACP system priority. See Setting a Name for a Static LAG.
3. You can change the LACP port definitions (port mode and priority). See Enabling and Configuring an Interface for LACP Aggregation.

Table 7-3 lists the LACP configuration commands, used for configuring dynamic links.

Table 7-3 LACP Configuration Commands

Command	Description
link-aggregation lacp enable/disable	Enables/disables LACP on the switch.
link-aggregation lacp system-priority	Sets the LACP system priority to the specified value.
link-aggregation lacp	Enables the configured interface to be added to a LAG or to be removed from a LAG dynamically by LACP.

Enabling/Disabling LACP Globally

The **link-aggregation lacp enable** command, in Protocol Configuration mode, globally enables LACP on the switch and allows configuration of global and per interface LACP parameters.

The **link-aggregation lacp disable** command, in Protocol Configuration mode, globally disables LACP on the switch and blocks configuration of global and per interface LACP parameters.

By default, LACP is disabled.

Command Syntax

```
device-name(cfg protocol)#link-aggregation lacp {enable | disable}
```

Argument Description

enable	Enables LACP.
disable	Disables LACP.

Specifying the System Priority

The **link-aggregation lacp system-priority** command, in Protocol Configuration mode, sets the LACP system priority to the specified value. The **no** form of this command sets the LACP system priority to the default value.

If a value is not specified, the command causes the current LACP system priority value to be displayed.

By default, the LACP system priority is 32768.

Command Syntax

```
device-name(cfg protocol)#link-aggregation lacp system-priority [<priority>]
device-name(cfg protocol)#no link-aggregation lacp system-priority
```

Argument Description

priority	Priority value, in the range 1 (highest priority) to 65535 (lowest priority).

Example

The following command sets the LACP system priority to 1 (the highest priority).

```
device-name(cfg protocol)#link-aggregation lacp system-priority 1
device-name(cfg protocol)#link-aggregation lacp system-priority
System priority = 1
```

Enabling and Configuring an Interface for LACP Aggregation

The **link-aggregation lacp** command, in Interface Configuration mode, enables the configured interface to be added to or removed from a LAG dynamically by the LACP. It also sets LACP parameters. The **no** form of the command disables LACP on the configured interface. The **no link-aggregation lacp port-priority** command resets the LACP priority of the configured interface to the default value.

If **port priority** is specified without a value, the command shows the current value.

If no optional arguments are entered and the configured interface is not LACP-enabled, the interface is configured with default argument values. If the interface is LACP-enabled, only explicitly entered optional arguments take effect.

When an interface is set to LACP **passive** mode, it will not start to exchange LACP frames until it receives such frames from the remote switch.

When an interface is set to LACP **active** mode, it will send LACP frames periodically (every 30 seconds). The exchange of LACP frames starts when the remote side answers.

By default, the LACP port is active with priority is 32768.

Command Syntax

```
device-name(config-if UU/SS/PP)# link-aggregation lacp [active | passive]
[port-priority [<priority>]]

device-name(config-if UU/SS/PP)#no link-aggregation lacp port-priority
device-name(config-if UU/SS/PP)#no link-aggregation
```

Argument Description

active	Enable LACP in active mode (default).
passive	Enable LACP in passive mode.
port-priority <priority>	The port priority value, in the range <1-65535>.

Specifying the STP/RSTP/MSTP Port Priority

STP/RSTP/MSTP port priority can be specified for aggregate ports in the same way as for normal ports. For details, refer to the respective (STP/RSTP/MSTP) chapter.

Specifying the STP/RSTP/MSTP Path Cost

STP/RSTP/MSTP path cost can be specified for aggregate ports in the same way as for normal ports. For details, refer to the respective (STP/RSTP/MSTP) chapter.

Displaying Link Aggregation Groups

Table 7-4 lists the commands to display the static LAG and LACP configuration.

Table 7-4 Commands to Display the Static LAG and LACP Configuration

Command	Description
show interface link-aggregation	Displays the Link Aggregation Groups configuration.
show link-aggregation lacp	Displays a list of all LACP-enabled interfaces in the system with the configured LACP parameters.

Displaying the Link Aggregation Groups

The **show interface link-aggregation** command, in Privileged (Enable) mode, displays the link aggregation groups in the system, as specified by the command arguments. If no argument is specified, the list includes all static and dynamic link aggregation groups.

NOTE

The show link aggregation command replaces the show trunk command. The show trunk command is also supported.

Command Syntax

```
device-name#show interface link-aggregation [static | dynamic | id <num>]
```

Argument Description

static	Displays only the statically defined link aggregation groups.
dynamic	Displays only the dynamic link aggregation groups, created by LACP.
id <num>	Displays the link aggregation group that is specified by the ID number (Not used in this version of the switch).

Example

```
device-name#show interface link-aggregation
==========+========+================+====================
Aggregate |Type    | Management Name | Ports              |
----------+--------+----------------+--------------------+
 AG01     | static | TRUNK1          | 1/1/3,1/1/5        |
 AG03     | LACP   | LACP3           | 1/1/14-1/1/16      |
==========+========+================+====================
```

Displaying the LACP Interfaces

The **show link-aggregation lacp** command, in Privileged (Enable) mode, displays a list of all LACP enabled interfaces on the switch with the configured LACP parameters.

Command Syntax

```
device-name#show link-aggregation lacp
```

Example

```
device-name#show link-aggregation lacp
System ID       = 00 a0 12 02 02 02
System priority = 32768
========+========+=======+=========
  Port   |  Mode  |  Key  |  Prty  |
--------+--------+-------+--------+
 1/1/1   | active |     3 | 32768  |
 1/1/2   | active |     3 | 32768  |
 1/1/3   | active |     3 | 32768  |
========+========+=======+=========
```

Configuration Examples

Simple LACP Configuration

The following example establishes dynamic link aggregation between two switches, as shown Figure 7-2.

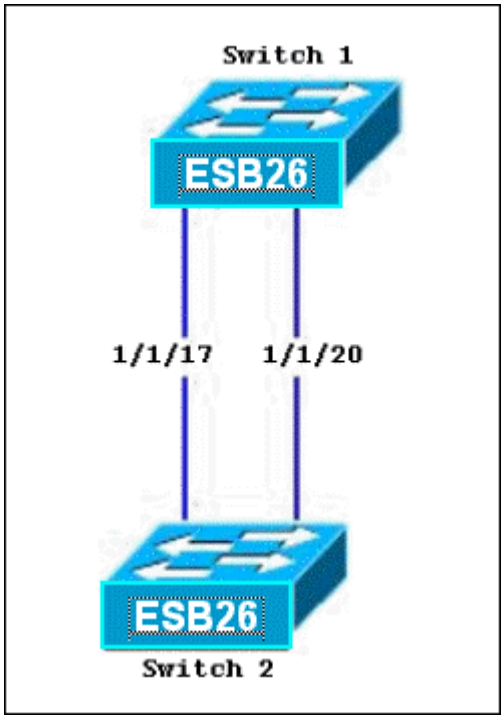


Figure 7-2: Example of LAG Containing Two Ports

On each of the two switches, LACP is enabled in active mode on interfaces 1/1/17 and 1/1/20 as an aggregated link. The configuration of Switch2 is identical to that of Switch1.

1. Display the LACP status:

```
device-name#show link-aggregation lacp
    LACP disabled on the system
```

2. Enter into Protocol Configuration mode and enable the LACP on switch 1:

```
device-name#configure terminal
device-name(config)#protocol
device-name(cfg protocol)#link-aggregation lacp enable
device-name(cfg protocol)#end
```

3. Display the LACP configuration:

```
device-name#show link-aggregation lacp
System ID       = 00 00 02 03 04 05
System priority = 32768
No LAC ports configured
```

4. Enable LACP on interface 1/1/17:

```
device-name#configure terminal
device-name(config)#interface 1/1/17
device-name(config-if 1/1/17)#link-aggregation lacp
```

5. Enable LACP on interface 1/1/20:

```
device-name(config-if 1/1/17)#interface 1/1/20
device-name(config-if 1/1/20)#link-aggregation lacp
device-name(config-if 1/1/20)#end
```

6. Display the LACP configuration

```
device-name#show link-aggregation lacp
System ID       = 00 00 02 03 04 05
System priority = 32768
========+========+=======+=========
  Port  |  Mode  |  Key  |  Prty  |
--------+--------+-------+--------+
 1/1/17 | active |     9 | 32768  |
 1/1/20 | active |     8 | 32768  |
========+========+=======+=========
```

7. If there is a link between the switches, the following results on each switch will be displayed:

```
device-name#show interface link-aggregation
==========+========+=================+====================
Aggregate |Type    | Management Name | Ports               |
----------+--------+-----------------+--------------------+
 AG09     | LACP   | LACP9           | 1/1/17,1/1/20      |
==========+========+=================+====================
```

Complex LACP Configuration

The following example establishes two dynamic link aggregation groups between three switches, as shown in Figure 7-3.

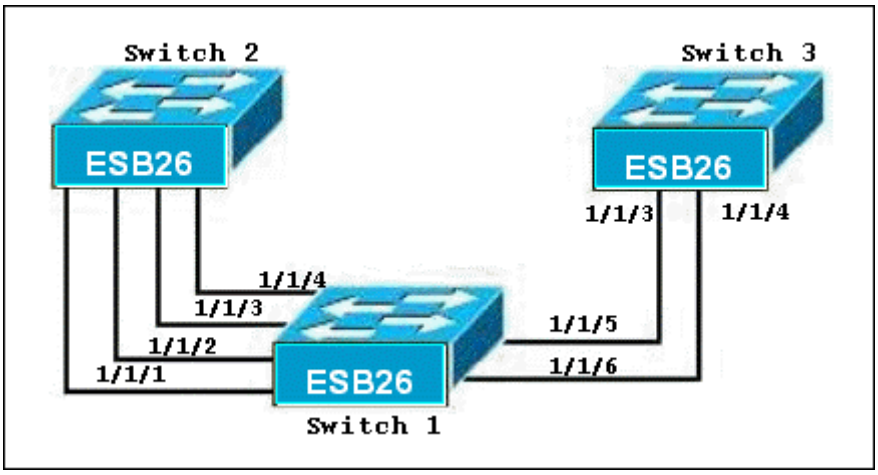


Figure 7-3: Example of Two LAGs Configured on the Same Switch

Configuring Switch 1:

On **Switch 1**, LACP is enabled in active mode on the following interfaces:

- 1/1/1, 1/1/2, 1/1/3 and 1/1/4, as an aggregated link to Switch 2;
- 1/1/5 and 1/1/6, as an aggregated link to Switch 3.

1. Enter into Protocol Configuration mode and enable the LACP on switch 1:

```
Switch1#configure terminal
Switch1(config)#protocol
Switch1(cfg protocol)#link-aggregation lacp enable
Switch1(cfg protocol)#end
```

2. Display the LACP configuration:

```
Switch1#show link-aggregation lacp
System ID       = 00 00 02 03 04 05
System priority = 32768
No LAC ports configured
```

3. Enable LACP on interfaces 1/1/1, 1/1/2, 1/1/3, 1/1/4, 1/1/5 and 1/1/6:

```
Switch1(config)#interface 1/1/1
Switch1(config-if 1/1/1)#link-aggregation lacp
Switch1(config-if 1/1/1)#interface 1/1/2
Switch1(config-if 1/1/2)#link-aggregation lacp
Switch1(config-if 1/1/2)#interface 1/1/3
Switch1(config-if 1/1/3)#link-aggregation lacp
Switch1(config-if 1/1/3)#interface 1/1/4
Switch1(config-if 1/1/4)#link-aggregation lacp
Switch1(config-if 1/1/4)#interface 1/1/5
Switch1(config-if 1/1/5)#link-aggregation lacp
Switch1(config-if 1/1/5)#interface 1/1/6
Switch1(config-if 1/1/6)#link-aggregation lacp
Switch1(config-if 1/1/6)#end
```

4. Display the LACP configuration:

```
Switch1#show link-aggregation lacp
System ID       = 00 00 02 03 04 05
System priority = 32768
========+========+=======+=========
  Port  |  Mode  |  Key  |  Prty  |
--------+--------+-------+--------+
 1/1/1  | active |     1 | 32768  |
 1/1/2  | active |     1 | 32768  |
 1/1/3  | active |     1 | 32768  |
 1/1/4  | active |     1 | 32768  |
 1/1/5  | active |     9 | 32768  |
 1/1/6  | active |     9 | 32768  |
========+========+=======+=========
```

Configuring Switch 2:

On **Switch 2**, LACP is enabled in active mode on interfaces 1/1/1, 1/1/2, 1/1/3 and 1/1/4, as an aggregated link to Switch 1.

1. Enter into Protocol Configuration mode and enable the LACP on switch 2:

```
Switch2#configure terminal
Switch2(config)#protocol
Switch2(cfg protocol)#link-aggregation lacp enable
Switch2(cfg protocol)#end
```

2. Display the LACP configuration:

```
Switch2#show link-aggregation lacp
System ID       = 00 a0 12 05 3a 80
System priority = 32768
No LAC ports configured
```

3. Enable LACP on interfaces 1/1/1, 1/1/2, 1/1/3 and 1/1/4:

```
Switch2#configure terminal
Switch2(config)#interface 1/1/1
Switch2(config-if 1/1/1)#link-aggregation lacp
Switch2(config-if 1/1/1)#interface 1/1/2
Switch2(config-if 1/1/2)#link-aggregation lacp
Switch2(config-if 1/1/2)#interface 1/1/3
Switch2(config-if 1/1/3)#link-aggregation lacp
Switch2(config-if 1/1/3)#interface 1/1/4
Switch2(config-if 1/1/4)#link-aggregation lacp
Switch2(config-if 1/1/4)#end
```

4. Display the LACP configuration:

```
Switch2#show link-aggregation lacp
System ID       = 00 a0 12 05 3a 80
System priority = 32768
========+========+=======+=========
  Port  |  Mode  |  Key  |  Prty  |
--------+--------+-------+--------+
 1/1/1  | active |     1 | 32768  |
 1/1/2  | active |     1 | 32768  |
 1/1/3  | active |     1 | 32768  |
 1/1/4  | active |     1 | 32768  |
========+========+=======+=========
```

Configuring Switch 3:

On **Switch 3**, LACP is enabled in active mode on interfaces 1/1/3 and 1/1/4, as an aggregated link to Switch 1.

1. Enter into Protocol Configuration mode and enable the LACP on switch 3:

```
Switch3#configure terminal
Switch3(config)#protocol
Switch3(cfg protocol)#link-aggregation lacp enable
Switch3(cfg protocol)#end
```

2. Display the LACP configuration:

```
Switch3#show link-aggregation lacp
System ID       = 00 a0 12 10 94 c0
System priority = 32768
No LAC ports configured
```

3. Enable LACP on interfaces 1/1/3 and 1/1/4:

```
Switch3#configure terminal
Switch3(config)#interface 1/1/3
Switch3(config-if 1/1/3)#link-aggregation lacp
Switch3(config-if 1/1/3)#interface 1/1/4
Switch3(config-if 1/1/4)#link-aggregation lacp
Switch3(config-if 1/1/4)#end
```

4. Display the LACP configuration:

```
Switch3#show link-aggregation lacp
System ID       = 00 a0 12 10 94 c0
System priority = 32768
=========+========+=======+=========
  Port   |  Mode  |  Key  |  Prty  |
---------+--------+-------+--------+
 1/1/3   | active |     5 | 32768  |
 1/1/4   | active |     5 | 32768  |
=========+========+=======+=========
```

After the LACP operation the following results on each switch will be displayed.

Switch 1:

```
Switch3#show interface link-aggregation
==========+========+================+====================
Aggregate |Type    | Management Name | Ports              |
----------+--------+----------------+--------------------+
 AG01     | LACP   | LACP1           | 1/1/1-1/1/4        |
 AG09     | LACP   | LACP9           | 1/1/5,1/1/6        |
==========+========+================+====================
```

Sswitch 2:

```
Switch2#show interface link-aggregation
==========+========+================+====================
Aggregate |Type    | Management Name | Ports              |
```

```
AG01      | LACP    | LACP1           | 1/1/1-1/1/4
==========+=========+=================+====================
```

Switch 3:

```
Switch3#show interface link-aggregation
==========+========+=================+====================
Aggregate |Type    | Management Name | Ports              |
----------+--------+-----------------+--------------------+
 AG05     | LACP   | LACP5           | 1/1/3-1/1/4        |
==========+========+=================+====================
```

Example of Static Link Aggregation with RSTP

The following example shows how to establish two static link aggregation groups between two switches with fast Ethernet interfaces, as shown in Figure 7-4. This setup requires a mechanism such as the Rapid Spanning Tree algorithm to prevent the two LAGs from forming a loop. For more information on the Rapid Spanning Tree algorithm, see "RSTP (Rapid Spanning Tree Protocol)".

The configuration of Switch2 is identical to that of Switch1. However, there are differences in the display of the RSTP configuration parameters, since RSTP automatically selects one switch (Switch 1 in our case) as the root bridge, and the other switch (Switch 2 in our case) as the designated bridge. This difference is reflected in the results of the **show rapid-spanning-tree** command, when applied to both switches.

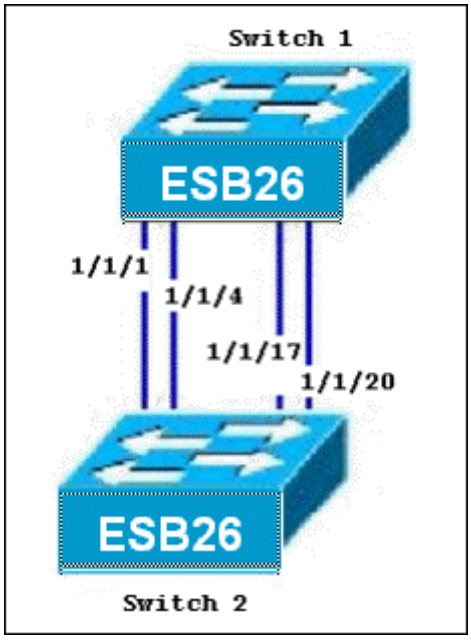


Figure 7-4: Example of Two Static LAGs with RSTP

Configuring Switch 1:

1. Enabling RSTP:

```
Switch1#configure terminal
```

```
Switch1(config)#protocol
Switch1(cfg protocol)#rapid-spanning-tree enable
Switch1(cfg protocol)#end
```

2. Enabling Static LAG on interfaces 1/1/1 and 1/1/4

```
Switch1#configure terminal
Switch1(config)#interface 1/1/1
Switch1(config-if 1/1/1)#link-aggregation static id 1
Switch1(config-if 1/1/1)#interface 1/1/4
Switch1(config-if 1/1/4)#link-aggregation static id 1
```

3. Enabling Static LAG on interfaces 1/1/17 and 1/1/20

```
Switch1(config-if 1/1/4)#interface 1/1/17
Switch1(config-if 1/1/17)#link-aggregation static id 3
Switch1(config-if 1/1/17)#interface 1/1/20
Switch1(config-if 1/1/20)#link-aggregation static id 3
Switch1(config-if 1/1/20)#end
```

Displaying the Configuration on Switch 1:

1. Displaying the static LAG configuration:

```
Switch1#show interface link-aggregation static
=========+======+======================+======================
Aggregate| Type | Management Name       | Ports
---------+------+----------------------+----------------------
  AG01   |static|TRUNK1                |1/1/1,1/1/4
  AG03   |static|TRUNK3                |1/1/17,1/1/20
```

2. Displaying the RSTP parameter settings and Rapid-Spanning-Tree topology:

```
Switch1#show rapid-spanning-tree
Rapid spanning tree     = enabled
ProtocolSpecification   = ieee8021w
Priority                = 32768
TimeSinceTopologyChange = 41 (Sec)
TopChanges              = 2
DesignatedRoot          = This bridge is the root
MaxAge                  = 20 (Sec)
HelloTime               = 2  (Sec)
ForwardDelay            = 15 (Sec)
BridgeMaxAge            = 20 (Sec)
BridgeHelloTime         = 2  (Sec)
BridgeForwardDelay      = 15 (Sec)
TxHoldCount             = 3
MigrationTimer          = 3  (Sec)
DetectLineCRCReconfig   = disabled

================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge|DPrt|FwrdT
--------+---+--------+-----+---------+---------+-----------------+----+-----
AG01     128 Designat frwrd       10      0    32768.00A0121102A3 128.88   1
AG03     128 Designat frwrd       10      0    32768.00A0121102A3 128.90   1
```

Displaying the Configuration on Switch 2 (After Configuring as Described for Switch 1):

1. Display the static LAG configuration:

```
Switch2#show interface link-aggregation static
=========+======+======================+======================
Aggregate| Type | Management Name       | Ports
---------+------+----------------------+----------------------
  AG01   |static|TRUNK1                |1/1/1,1/1/4
  AG03   |static|TRUNK3                |1/1/17,1/1/20
```

2. Display the RSTP parameter settings and Rapid-Spanning-Tree topology:

```
Switch2#show rapid-spanning-tree
Rapid spanning tree     = enabled
ProtocolSpecification   = ieee8021w
Priority                = 32768
TimeSinceTopologyChange = 4 (Sec)
TopChanges              = 1
DesignatedRoot          = 32768.00:A0:12:11:02:A3
RootPort                = AG01
RootCost                = 10
MaxAge                  = 20 (Sec)
HelloTime               = 2  (Sec)
ForwardDelay            = 15 (Sec)
BridgeMaxAge            = 20 (Sec)
BridgeHelloTime         = 2  (Sec)
BridgeForwardDelay      = 15 (Sec)
TxHoldCount             = 3
MigrationTimer          = 3  (Sec)
DetectLineCRCReconfig   = disabled

================================================================================
Port  |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt |FwrdT
------+---+--------+-----+---------+---------+------------------+-----+-----
AG01   128 Root     frwrd  10       0          32768.00A0121102A3 128.88  1
AG03   128 Altern   discr  10       0          32768.00A0121102A3 128.90  1
```

8. Traffic Monitoring

Introduction

Traffic monitoring extends the monitoring capabilities of existing network analyzers in a switched Ethernet environment. Traffic can be monitored on switch's ports and VLANs by configuring another port to "mirror" the traffic on the ports or VLANs you want to monitor. By attaching an analyzer to the mirror port, the system administrator can observe the traffic on the monitored ports and analyze the traffic on the network.

Feature Overview

A local monitor session is an association of a destination port with source ports and source VLANs. You configure monitor sessions by using parameters that specify the source of network traffic to the monitor.

For example, in Figure 8-1, all traffic on ports 1/1/1, 1/1/2, 1/1/3, 1/1/4, 1/1/10 and 1/1/12 is monitored by the port 1/1/13. A network analyzer on port 1/1/13 receives all network traffic from these ports without being physically attached to port 1/1/13.

Figure 8-2 shows an example of a monitor session. All traffic on VLAN 100 and VLAN 101 (the source VLANs) is monitored by the port 1/1/4 (the destination port). A network analyzer on port 1/1/4 receives the outgoing network traffic on the VLANs.

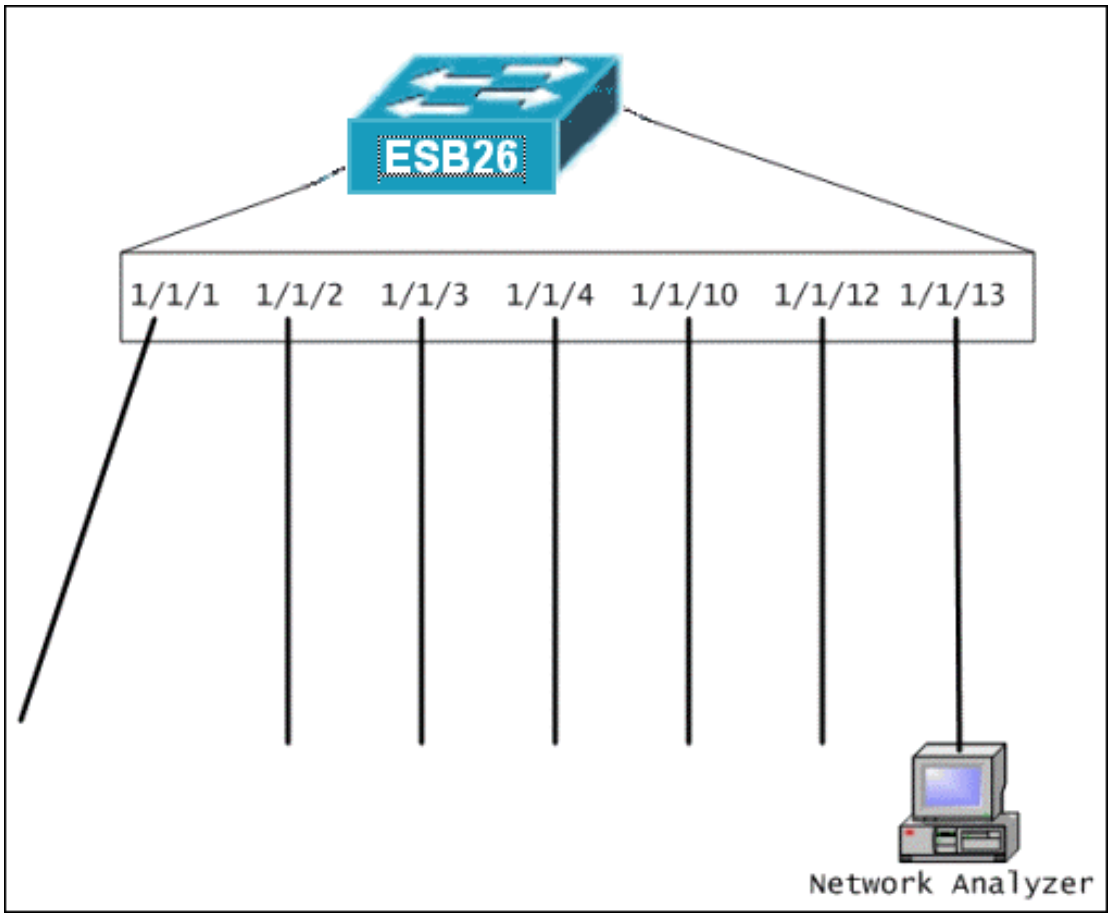


Figure 8-1 Example of Monitor Session Configuration on Interface

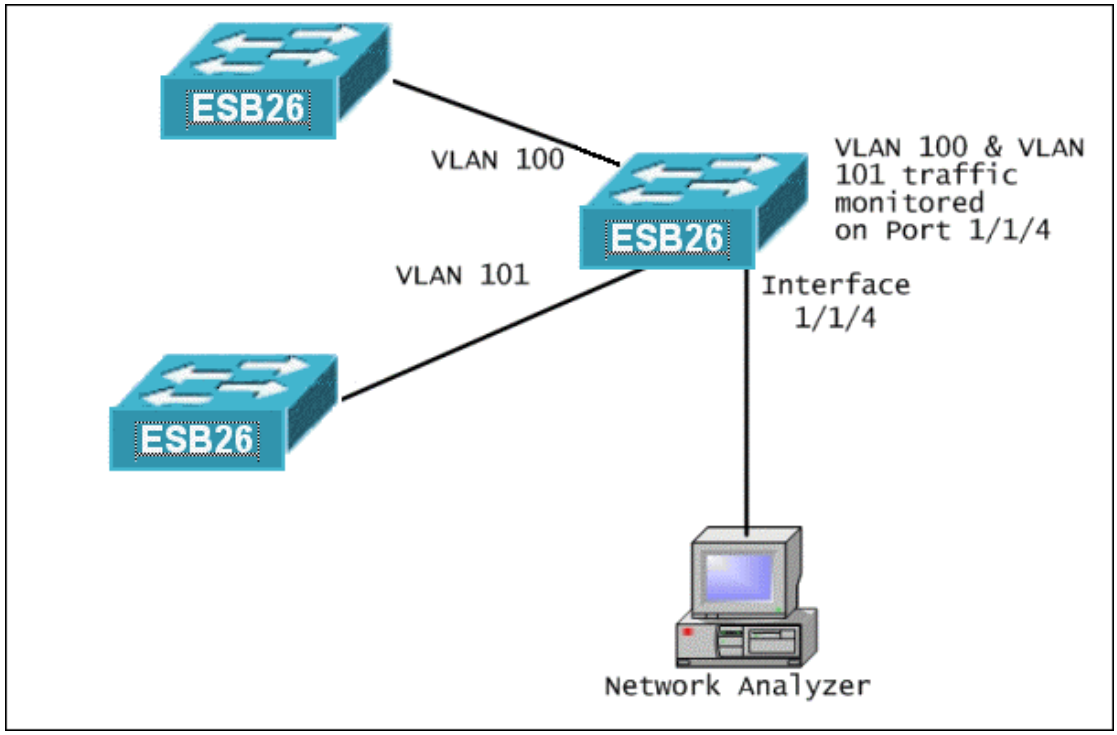


Figure 8-2 Example of Monitor Session Configuration on VLANs

Traffic Types

A monitor session includes the following traffic types:

- **Receive (Rx)** - The goal of receive (or ingress) monitoring is to monitor the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port that monitors the session. At the destination port, if the packet is tagged, it will appear with the 802.1Q header.
- **Transmit (Tx)** - The goal of transmit (or egress) monitor session is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that monitor session. The copy is provided after the packet is modified.

Source Port

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis. In a single local monitor session, you can monitor source port traffic such as received (Rx), transmitted (Tx), or bidirectional.

On the Rx the switch supports any number of source ports up to the maximum number of available ports on the switch, and any number of source VLANs up to the maximum number of VLANs supported.

On the Tx the switch supports up to eight source ports.

A source port has the following characteristics:

- It can be any port type (for example, Fast Ethernet, Gigabit Ethernet, link aggregation group and so forth).
- It cannot be a destination port.
- Each source port can be configured with a direction (Rx, Tx, or both) to monitor.
- Source ports can be in the same or different VLANs.

For VLAN monitor sources, all active ports in the source VLAN are included as source ports.

Destination Port

Each local monitor session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports and VLANs.

The destination port has the following characteristics:

- It must reside on the same switch as the source port.
- It can be any Ethernet physical port.
- It cannot be a source port.

NOTE  The destination port is limited to its capacity. All traffic that exceeds the port's capacity will be dropped.

Supported Standards, MIBs and RFCs

Standards

No standards are supported by this feature.

MIBs

No MIBs are supported by this feature.

RFCs

No RFCs are supported by this feature.

Prerequisites

You cannot define different monitoring directions (transmit, receive) for both a VLAN list and an interface list concurrently (such as the transmit source defined to be a VLAN list and the receive source defined to be an interface list in the same monitoring session).

Up to of eight ports can be monitored on the transmitted traffic. If a VLAN list is monitored, only the first eight ports will be monitored.

The monitored VLANs must be defined before adding them to the monitor session.

The monitor session will start to function only when the analyzer port (destination) is set by the **monitor session destination** command in Global Configuration mode.

When activating a monitor session on a port list, the analyzer port (destination) is automatically removed from all the VLANs in which it was a member and automatically added as an untagged member to all the VLANs in which the monitored ports are members.

When activating monitor session on VLAN list, the analyzer port (destination) is automatically removed from all the VLANs it was member in, and automatically as untagged member added to all the monitored VLANs.

When the monitor session is disabled, the destination port is automatically removed from all the VLANs and added as an untagged member to the default VLAN (VLAN ID 1).

Do not add the analyzer port to VLANs. It can affect the monitor session operation.

Default Traffic Monitoring Configuration

Table 8-1 shows the default traffic monitoring configuration.

Table 8-1 Default Traffic Monitoring Configuration

Parameter	Default Value
Monitor Session	Disabled

Configuring and Displaying Monitor Session

Table 8-2 lists the monitor session commands.

Table 8-2 Monitor Session Commands

Command	Description
monitor session	Enables a port monitor session.
show monitor session	Displays the monitor session configuration.

Setting Monitor Session

The **monitor session** command, in Global Configuration mode, starts a new traffic monitoring session. Use the **no** form of this command to remove the monitor session or to remove the source VLANs.

To add or delete VLANs to or from an existing traffic monitoring session you need to disable the monitor session definitions and to create new monitor session.

Command Syntax

```
device-name(config)#monitor session {rx|tx} destination interface UU/SS/PP
device-name(config)#monitor session {rx|tx} source {vlan VLAN-LIST|interface PORT-LIST}
device-name(config)#no monitor session {rx|tx}
```

Argument Description

rx	Sets the session to monitor ingress traffic.
tx	Sets the session to monitor egress traffic.
interface UU/SS/PP	The destination interface for a monitor session.
vlan VLAN-LIST	List of source VLAN IDs. Use commas as separators and hyphens to indicate sub-ranges (e.g. 5-10,100). The VLAN IDs are in the range <1-4094>.
interface PORT-LIST	List of source interfaces. Use commas as separators and hyphens to indicate sub-ranges (e.g. 1/1/1-1/1/5, 1/1/20).

Example

The following example shows how to configure a monitor session to monitor ingress traffic on multiple source VLANs.

```
device-name(config)#monitor session rx source vlan 5-10,100
device-name(config)#monitor session rx destination 1/1/3
```

Displaying Monitor Session Configuration

The **show monitor session** command, in Privileged (Enable) mode, displays the monitor session configuration.

Command Syntax

```
device-name#show monitor session
```

Example

```
device-name(config)#monitor session rx destination interface 1/1/8
device-name(config)#monitor session rx source interface 1/1/10-1/1/20
device-name(config)#end
device-name#show monitor session
================================================
 Monitor | Analyzer | Source   | Monitored Source
---------+----------+---------+------------------
Transmit |          |         |
Receive  |  1/1/8   |  ports  |  1/1/10-1/1/20
```

Configuration Examples

Configuration Example for Monitor Session on Ports

The following example, based in Figure 8-1, shows how to configure the monitor session on ports. Interface 1/1/13 mirrors the traffic on interfaces 1/1/1, 1/1/2, 1/1/3, 1/1/4, 1/1/10 and 1/1/12. The traffic is monitored both for Rx and Tx:

```
device-name(config)#monitor session rx destination interface 1/1/13
device-name(config)#monitor session tx destination interface 1/1/13
device-name(config)#monitor session rx source interface 1/1/1-1/1/4,
1/1/10,1/1/12
device-name(config)#monitor session tx source interface 1/1/1-
1/1/3,1/1/10,1/1/12
device-name(config)#end
device-name#show monitor session
================================================
 Monitor | Analyzer | Source   | Monitored Source
---------+----------+---------+------------------
 Transmit|  1/1/13  |  ports  |  1/1/1-1/1/4,1/1/10,1/1/12

 Receive |  1/1/13  |  ports  |  1/1/1-1/1/4,1/1/10,1/1/12
```

Configuration Example for Monitor Session on VLAN

The following example is based in Figure 8-2 and shows how to configure the monitor session on VLAN, interface 1/1/4 is mirroring the traffic on VLANs 100 and 101. The traffic is monitored both for Rx and Tx.

```
device-name(config)#monitor session rx destination interface 1/1/4
device-name(config)#monitor session tx destination interface 1/1/4
device-name(config)#monitor session rx source vlan 100-101
device-name(config)#monitor session tx source vlan 100-101
device-name(config)#end
device-name#show monitor session
================================================
 Monitor | Analyzer | Source  | Monitored Source
---------+----------+---------+------------------
 Transmit|  1/1/4   |  vlans  |  100,101

 Receive |  1/1/4   |  vlans  |  100,101
```

9. Resilient Link

Introduction

A resilient link provides a secondary backup link to protect a network against failure of an individual link or device. The backup link becomes active only if a failure on the main link occurs. A resilient link comprises a resilient link pair that contains a main link and a standby link. If the main link fails, the standby link immediately takes over the task of the main link.

Under normal network conditions, the main link carries network traffic. If a signal loss is detected, the device immediately enables the standby link for carrying the data. The standby port assumes the profile and carries the network traffic of the main port.

A port is said to be *preferred* if it is always the main port as long as it has the link. Traffic will be switched back to the main port as soon as its connection is recovered. The preferred port can be established in several ways:

- The port with the higher bandwidth gets the preference.
- One port is configured as preferred by the **prefer port** command (described below).

Active port refers to the current active port. You can determine the active port manually, using the **active port** command (described below) only if the preferred port has not been established. By default (if you have not configured a preferred or active port, and the two ports have the same bandwidth capacity), the active port is the first port you configure by the **ports** command (described below).

Switchover time to the backup link is less than 1 second, ensuring that no session timeouts take place and avoiding system timeouts.

NOTES

- Resilient links are incompatible with a spanning tree or trunk port.
- When adding a new port to an existing trunk, the VLAN of the trunk ports is synchronized.
- Both links of the resilient link must be included in the same VLANs, if there are any.
- Both resilient link ports must have the same default VLAN.

Configuring and Displaying a Resilient Link

Resilient link Configuration and Viewing Commands

Command	Description
resilient-link	Enters a specific resilient link configuration mode.
ports	Adds a port pair as a resilient link.

prefer port	Designates the preferred port of the resilient link.
active port	Designates the active port of the resilient link.
show	Displays a table of the configured resilient links.
show counter	Produces a table showing how many swaps each resilient link has undergone in the current session.
show resilient-links	Displays a table of the configured resilient links.
show resilient-links counter	Produces a table showing how many swaps each resilient link has undergone in the current session.
shutdown	Disables the interface (receiving, forwarding and learning). For a detailed description of this command, refer to "Ethernet Interface Configuration"

Description of Commands

resilient-link

The **resilient-link** command, in Global Configuration mode, opens a specified Resilient-link Configuration mode for settings of the specified resilient link.

When applied in a specified Resilient-link Configuration mode, the **resilient-link** command changes the editing focus from the current resilient link to the newly specified resilient link.

The **no** form of the **resilient-link** command removes the specified resilient link from the list of defined resilient links. The **no** form is also applied in Configuration mode.

The **resilient-link** command is disabled if Spanning Tree is enabled.

Command Syntax

```
device-name(config)#resilient-link <N>
```

OR

```
device-name(config-resil-link N1)#resilient-link <N2>
```

Removing a resilient link:

```
device-name(config)#no resilient-link <N>
```

Argument Description

N, N1, N2	Any number in the range <1-32>

Examples

1. Opening a specified Resilient-link Configuration mode:

```
device-name(config)#resilient-link 1
device-name(config-resil-link 1)#
```

2. Changing the mode to another resilient link:

```
device-name(config-resil-link 1)#resilient-link 2
device-name(config-resil-link 2)#
```

3. Removing a specified resilient link from the list of defined resilient links:

```
device-name(config)#no resilient-link 1
```

ports

The **ports** command, in Resilient-link Configuration mode, adds a port pair as a resilient link. This adds a new resilient link to a list of already defined resilient links. Ports are defined in unit/slot/port notation.

The operation is allowed if the current resilient link hasn't been configured yet. Otherwise, if you want to replace ports of an existing resilient link, proceed as follows:

Step 1. Return to global Configuration mode.

Step 2. Use the **no resilient-link** command, specifying the number of the resilient link to be reconfigured.

Step 3. Use the **resilient-link** command, again specifying the number of the resilient link to be reconfigured.

Step 4. Use the **ports** command to define the resilient link with the new pair of ports.

NOTES

If one of the added ports belongs to a VLAN(s), the other port will be included in the same VLAN(s) with the same tagging.

If any of the ports belonging to a resilient link will be included into any VLAN in the future, the other port of the resilient link will automatically be included in the VLAN.

The ports command is rejected if any of the following conditions is true:

- Any of the added ports belongs to a trunk.
- Any attempt to include a port of a resilient link into a trunk will be rejected.
- The resilient link ports do not have the same default VLAN.

Command Syntax

```
device-name(config-resil-link N)#ports UU1/SS1/PP1 UU2/SS2/PP2
```

Argument Description

UU1/SS1/PP1	The first resilient link port number
UU2/SS2/PP2	The second resilient link port number

Example

Adding the ports pair 1/1/4 and 1/1/5 to the list of resilient links, as resilient link #3:

```
device-name(config)#resilient-link 3
device-name(config-resil-link 3)#ports 1/1/4 1/1/5
```

prefer port

The **prefer port** command, in Resilient-link Configuration mode, sets one of the ports of the resilient link as preferred.

A port is said to be *preferred* if it is always the main port as long as it has the link. Traffic will be switched back to the main port as soon as its connection is recovered. The preferred port can be established in several ways:

- The port with the higher bandwidth gets the preference.
- One port is configured as preferred by the **prefer port** command.

Use the **no prefer port** command to cancel the preference (unless the ports has a higher bandwidth capacity).

Command Syntax

```
device-name(config-resil-link N)#prefer port UU/SS/PP
device-name(config-resil-link N)#no prefer port
```

Argument Description

UU/SS/PP	The preferred port number.

Example

After having configured ports 1/1/4 and 1/1/5 as resilient link #3, preferring port 1/1/4:

```
device-name(config-resil-link 3)#prefer port 1/1/4
```

active port

The **active port** command, in Resilient-link Configuration mode, switches the active port of the currently edited resilient link.

Active port refers to the current active port. You can determine the active port manually, using the **active port** command only if the preferred port has not been established. By default (if you have not configured a preferred or active port, and the two ports have the same bandwidth capacity), the active port is the first port you configure by the **ports** command (described above).

Command Syntax

```
device-name(config-resil-link N)#active port UU/SS/PP
```

Argument Description

UU/SS/PP	The active port number.

Example

Switching the active port of resilient link 3 to port 1/1/4:

```
device-name(config-resil-link 3)#active port 1/1/4
```

show

The **show** command, in Resilient-Link Configuration mode, displays a table of the configured resilient links. The table specifies the resilient-link ID numbers, the resilient link ports, which port is preferred (if any), and which port is currently active.

You can specify by ID number or by a range of ID numbers which configured resilient links to display. If no ID number is specified, all configured resilient links are displayed.

This command is identical in effect to the **show resilient-links** command in View mode or Privileged (Enable) mode, as described below.

Command Syntax

```
device-name(config-resil-link N)#show [N1|N1 N2]
```

Argument Description

N1	(Optional) ID number of resilient link to be displayed
N1 N2	(Optional) Range of ID numbers of resilient link to be displayed

Examples

1. Displaying information on all currently configured resilient links:

```
device-name(config-resil-link 1)#show
=========================================
| RLink | Port1 | Port2 | Prefer | Active |
+-------+-------+-------+--------+--------+
|   1   | 1/1/1 | 1/1/2 | Port 1 | Port 2 |
|   2   | 1/1/5 | 1/1/6 |        | Port 1 |
=========================================
```

2. Displaying information on resilient link #3:

```
device-name(config-resil-link 1)#show 3
=========================================
| RLink | Port1 | Port2 | Prefer | Active |
+-------+-------+-------+--------+--------+
|   3   | 1/1/3 | 1/1/4 |        |        |
=========================================
```

3. Displaying information on the configured resilient links in the range #1 to #4:

```
device-name(config-resil-link 1)#show 1 4
=========================================
| RLink | Port1 | Port2 | Prefer | Active |
+-------+-------+-------+--------+--------+
|   1   | 1/1/1 | 1/1/2 |        |        |
|   3   | 1/1/3 | 1/1/4 |        |        |
=========================================
```

show counter

The **show counter** command, in Resilient-link Configuration mode, produces a table showing how many swaps each resilient link has undergone in the current session.

You can specify by ID number or by a range of ID numbers which configured resilient links to display. If no ID number is specified, all configured resilient links are displayed.

This command is identical in effect to the **show resilient-links counter** command Privileged (Enable) mode, as described below.

Command Syntax

```
device-name(config-resil-link N)#show counter [N1|N1 N2]
```

Argument Description

N1	(Optional) ID number of resilient link to be displayed.
N1 N2	(Optional) Range of ID numbers of resilient link to be displayed.

Examples

1. Displaying the swap count on all currently configured resilient links:

```
device-name(config-resil-link 1)#show counter

======================
| RLink | Swap count |
+-------+------------+
|   1   |         7  |
|   3   |         0  |
|   5   |         3  |
======================
```

2. Displaying the swap count on all resilient link #5:

```
device-name(config-resil-link 1)#show counter 5

======================
| RLink | Swap count |
+-------+------------+
|   5   |         3  |
======================
```

3. Displaying the swap count on the configured resilient links in the range #1 to #4:

```
device-name(config-resil-link 1)#show counter 1 4

======================
| RLink | Swap count |
+-------+------------+
|   1   |         7  |
|   3   |         0  |
======================
```

show resilient-links

The **show resilient-links** command, in Privileged (Enable) mode, displays a table of the configured resilient links. The table specifies the resilient-link ID numbers, the resilient link ports, which port is preferred (if any), and which port is currently active.

You can specify by ID number or by a range of ID numbers which configured resilient links to display. If no ID number is specified, all configured resilient links are displayed.

This command is identical in effect to the **show** command in Resilient-link Configuration mode, as described above.

Command Syntax

```
device-name#show resilient-links [N1 | N1 N2]
```

Argument Description

N1	(Optional) ID number of resilient link to be displayed
N1 N2	(Optional) Range of ID numbers of resilient link to be displayed

Examples

1. Displaying information on all currently configured resilient links:

```
device-name#show resilient-links

=========================================
| RLink | Port1 | Port2 | Prefer | Active |
+-------+-------+-------+--------+--------+
|   1   | 1/1/1 | 1/1/2 | Port 1 | Port 2 |
|   2   | 1/1/5 | 1/1/6 |        | Port 1 |
=========================================
```

2. Displaying information on resilient link #3:

```
device-name#show resilient-links 3
=========================================
| RLink | Port1 | Port2 | Prefer | Active |
+-------+-------+-------+--------+--------+
|   3   | 1/1/3 | 1/1/4 |        |        |
=========================================
```

3. Displaying information on the configured resilient links in the range #1 to #4:

```
device-name#show resilient-links 1 4
=========================================
| RLink | Port1 | Port2 | Prefer | Active |
+-------+-------+-------+--------+--------+
|   1   | 1/1/1 | 1/1/2 |        |        |
|   3   | 1/1/3 | 1/1/4 |        |        |
=========================================
```

show resilient-links counter

The **show resilient-links counter** command, in Privileged (Enable) mode, produces a table showing how many swaps each resilient link has undergone in the current session.

You can specify by ID number or by a range of ID numbers which configured resilient links to display. If no ID number is specified, all configured resilient links are displayed.

This command is identical in effect to the **show counter** command in Resilient-link Configuration mode, as described above.

Command Syntax

```
device-name#show resilient-links counter [N1 | N1 N2]
```

Argument Description

N1	(Optional) ID number of resilient link to be displayed

N1 N2	(Optional) Range of ID numbers of resilient link to be displayed

Examples

1. Displaying the swap count on all currently configured resilient links:

```
device-name#show resilient-links counter

======================
| RLink | Swap count |
+-------+------------+
|   1   |         7  |
|   3   |         0  |
|   5   |         3  |
======================
```

2. Displaying the swap count on all resilient link #5:

```
device-name#show resilient-links counter 5

======================
| RLink | Swap count |
+-------+------------+
|   5   |         3  |
======================
```

3. Displaying the swap count on the configured resilient links in the range #1 to #4:

```
device-name#show resilient-links counter 1 4

======================
| RLink | Swap count |
+-------+------------+
|   1   |         7  |
|   3   |         0  |

======================
```

10. SNMP Server Configuration

Introduction

SNMP (Simple Network Management Protocol) is the Network management protocol that is used almost exclusively in TCP/IP networks. The Nokia ESB26 switch is fully manageable via SNMP.

Configuring and Displaying the SNMP Server Settings

SNMP Configuration Commands

In order to activate the SNMP agent and make a communication inside the SNMP entity (from the manager to the agent), proceed according to the following guidelines:

1. Change the SNMP engine-ID if the scheme for the engine-ID used in the network requires it. See Configuring the Agent Engine ID.
2. Enable the SNMP agent. See Enabling the SNMP Server.
3. Create views. See Defining SNMP Views.
4. Create groups. See Defining SNMP Groups.
5. Create the users. See Defining an SNMP User.
6. If you need to limit the managed communication for users according to access list criteria, see Displaying the Named Access Lists
7. The show **access-lists** command, in Privileged (Enable) mode, displays the defined named access lists.

Command Syntax

```
device-name#show access-lists
```

Example

The following example displays the defined rule for any routing protocol. The access list, named ***jiji,*** permits access from any source. The access list, named ***phone,*** permits all addresses from the range 34.34.34.6/16 that meet an exact match.

```
device-name(config)#access-list jiji permit any
device-name(config)#access-list phone permit 34.34.34.6/16
device-name#show access-lists
access-list jiji permit any
ccess-list phone permit 34.34.34.6/16
```

8. Assigning an Access List to a User.

NOTE You must configure your management system with the same parameters that are assigned to the users in the agent.

Table 10-1 lists the configuration commands for the SNMPv3 Agent.

Table 10-1 SNMPv3 Agent Configuration Commands

Command	Description
snmp-server engineID	Changes the agent's SNMP engine ID.
snmp-server enable	Enables the SNMP Server.
snmp-server view	Creates a view.
snmp-server group	Creates an SNMPv3 group and associates views to this group.
snmp-server user	Creates an SNMP v1, v2c or v3 user and associates it to a group.
snmp-server log-notify	Enables the SNMP notification log.
clear snmp-server log-notify	Clears the SNMP notification log.

Configuring the Agent Engine ID

The **snmp-server engineID** command, in Global Configuration mode, changes the engine ID. The **no** form of this command is returning the ID to its default value.

The engine ID is a string that contains an even number of characters, between 10 and 64 characters, that represent a hexadecimal number. Internally, this string is represented by a sequence of 5 to 32 whole bytes, each byte representing two hexadecimal digits. The user should enter an odd number of hexadecimal digits, otherwise the parser would pad the last byte with zeros in the byte's four most-significant bits. As a result, an extra zero will be inserted before the last digit. For example, if you enter the string 11223344556 (an odd number of characters), the agent's parser will interpret it as 0x112233445506.

You can set the SNMP Engine ID following a vendor-recommended scheme or your own rules. If you wish to change the engine ID it is recommended to set it before adding any users, and not to perform changes of the Engine ID once users are configured.

NOTE It is prohibited to have two SNMP entities in the management domain with the same Engine ID.

Changing of the Engine ID while there are users that use SNMPv3 authentication or using privacy and authentication will invalidate the keys and will require recalculation.

NOTE It is recommended to set the Engine ID first.

If you use third party MIB SNMP Managers, you should check the Engine ID configuration.

By default, the engine ID is 00 00 02 DB 03 [*MAC-ADDR*] 00 00, where [*MAC-ADDR*] represents the switch's MAC address.

Command Syntax

```
device-name(config)#snmp-server engineID ENGINE-ID
device-name(config)#no snmp-server engineID
```

Argument Description

ENGINE-ID	A string of 10 to 64 characters (represented internally by 5 to 32 bytes) that represents the agent's Engine ID as a hexadecimal number. Use an even number of characters in the range <0 – 9> and <a – f> (case-insensitive).

Example

The following example shows how to set the agent local **engineID** to 1234567890ABCD:

```
device-name(config)#snmp-server engineID 1234567890ABCD
```

Enabling the SNMP Server

The **snmp-server enable** command, in Global Configuration mode, enables the SNMP server. If the UDP port number is specified in the command, the agent will listen for incoming SNMP messages on this port. Otherwise, it will use the standard SNMP port 161. The **no** form of this command disables the SNMP server.

By default, the SNMP server is disabled.

NOTE If the SNMP server is disabled it can still be configured from the Command Line Interface, but it cannot respond to SNMP PDUs and cannot send traps.

Command Syntax

```
device-name(config)#snmp-server enable [<udp-port>]
device-name(config)#no snmp-server enable
```

Argument Description

udp-port	The number of the UDP port on which the SNMP server listens for messages. If the UDP port is not specified, the SNMP server listens for incoming messages on its default UDP port – 161. The range is <1-65535>.

Example

The following example shows how to enable the SNMP server on port 1021:

```
device-name(config)#snmp-server enable 1021
```

Defining SNMP Views

The **snmp-server view** command, in Global Configuration mode, defines the subset of all MIB objects accessible to the given view. This command includes or excludes a branch of the MIB tree in a view. The **no** form of the command removes the defined view.

The MIB definition represents a tree where each node in the tree is identified by a number. To identify a branch in the tree, the usual convention is to use a series of numbers separated by dots, where each number represents a node in the tree.

The view name is created if it does not exist. If the view definition exists, the defined subtree is added to the list of view families. If the Object ID already exists, it is replaced by the new data (type of rule and mask). The mask is optional and defines wildcard characters for matching multiple Object IDs. The mask is entered as a hexadecimal value, and is interpreted as a binary value. A binary '1' in the mask states that the Object ID at the corresponding position should match, a binary '0' states that the Object ID at the corresponding position is irrelevant – no match is required.

Command Syntax

```
device-name(config)#snmp-server view VIEW-NAME OID-TREE {included |
excluded} [MASK]
device-name(config)#no snmp-server view VIEW-NAME [OID-TREE]
```

Argument Description

VIEWNAME	The name of the View. The view name is limited to 32 characters.
OID-TREE	Starting point inside the MIB tree given in dot-notation.
included	The Object-ID is included in the view.
excluded	The Object-ID is excluded from the view.
MASK	Bit-mask defining OID wildcard.

Example 1

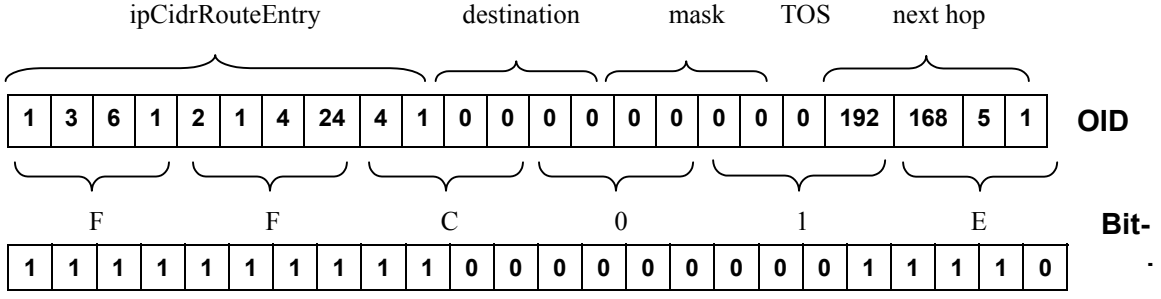
The following commands create the view ***MyView*** and add two rules to it.

- The first rule enables access to all Object IDs under the MIB-2 tree (all object identifiers that start with 1.3.6.1.2.1).
- The second rule disables access to the sysUpTime Object ID.

Grant or denial of access is determined by the most specific rule (with the longest match) that matches the object ID. When the agent decides whether to grant access to the Object ID 1.3.6.1.2.1.1.3 – both entered rules of ***MyView*** match the object. The second rule has a longer match to the view family and the result is that access is denied (by the **excluded** keyword).

```
device-name(config)#snmp-server view MyView 1.3.6.1.2.1 included
device-name(config)#snmp-server view MyView 1.3.6.1.2.1.1.3 excluded
```

Example 2



The following command grants access to all conceptual rows in *ipCidrRouteTable* that have next-hop 192.168.5.1. The destination, mask and the TOS entered in the OID have no match (the bits of the mask are '0' at these OIDs).

If an Object ID does not match any rule in a view, its access is denied.

```
device-name(config)#snmp-server view v1
1.3.6.1.2.1.4.24.4.0.0.0.0.0.0.0.0.192.168.5.1 include FFC01E
```

Example 3

The following command removes the specified view data. If the optional Object ID is not supplied, all the data of the view VIEWNAME will be deleted. If the user enters an Object ID (by name or dot-notation), then only the rule with the view family that matches the Object ID will be deleted.

```
device-name(config)#no snmp-server view VIEWNAME OID
```

Example 4

The following example shows how to delete the rule for the ***sysUpTime*** (1.3.6.1.2.1.1.3) view family (all other data of ***MyView*** is preserved):

```
device-name(config)#no snmp-server view MyView 1.3.6.1.2.1.1.3
```

Example 5

The following example shows how to delete all data for the view with name ***MyView***:

```
device-name(config)#no snmp view MyView
```

Defining SNMP Groups

The **snmp-server group** command, in Global Configuration mode, creates an SNMP group with a specified security model (v1, v2c or v3), and defines the access-right for this group by associating views to this group. If the security model is v3, you can specify the security level – *noAuth*, *Auth* or *AuthPriv*. The **no** form of the command deletes the SNMP group data. If you specify only the group name, all groups with that name will be removed, regardless of their security model and security level. If the security model and security level (if the model is v3) are specified, only the group matching all conditions is removed.

The Groups define the views that enable access for reading, writing, and notification. In SNMPv3, a user can participate in more than one group, provided that each group has a different security model. When a SNMPv3 PDU is received, it carries information about the user and the security model. The local configured group in which the user participates and the security model are defined by the information in the PDU.

Command Syntax

```
device-name(config)#snmp-server group NAME {v1 | v2c} read READ-VIEW write
WRITE-VIEW notify NOTIFY-VIEW
device-name(config)#no snmp-server group NAME [v1 | v2c]

device-name(config)#snmp-server group NAME v3 {auth | noauth | priv} read
READ-VIEW write WRITE-VIEW notify NOTIFY-VIEW
device-name(config)#no snmp-server group NAME [v3 {auth | noauth | priv}]
```

Argument Description

NAME	Configures a new SNMP group on the device. The name of the group is limited to 32 characters.
v1	Version 1 of the SNMP protocol.
v2c	Version 2 of the SNMP protocol.
v3	Version 3 of the SNMP protocol. Requires you to select an authentication level (auth, noauth or priv).
auth	Enables the Message Digest 5 (HMAC-MD5) or the Secure Hash Algorithm (HMAC-SHA) packet authentication.
noauth	Security level, which implies no authentication and no encryption of the PDUs. This is the default if no keyword is specified.
priv	Enables Data Encryption Standard (DES) packet encryption. Authentication is based on HMAC-MD5 or HMAC-SHA and CBC-DES encryption.
read READ-VIEW	A string (not to exceed 32 characters) that is the name of the view in which you can only view the contents of the agent.
write WRITE-VIEW	A string (not to exceed 32 characters) that is the name of the view in which you enter data and configure the contents of the agent.
notify NOTIFY-VIEW	A string (not to exceed 32 characters) that is the name of the view, which specifies what portion of the MIB database is accessible for notifications.

Example 1

```
device-name(config)#snmp-server group GR1 v3 auth read v3_read write
v3_write notify v3_read
```

Example 2

The following example shows how to delete the group named ***MyGroup***:

```
device-name(config)#no snmp-server group MyGroup
```

Example 3

The following example shows how to delete a group that is named ***MyGroup2***, and has security model v3 and security level *AuthPriv*. Note that if there are v1 and v2 groups named ***MyGroup2***, they will not be removed.

```
device-name(config)#no snmp-server group MyGroup2 v3 priv
```

Defining an SNMP User

The **snmp-server user** command, in Global Configuration mode, creates an SNMP local or remote user and associates it to a group. If the security model is v3, enter the security level for the user. The **no** form of the command removes the defined user and removes the user from its associated group.

For SNMPv3 users, if no security level is specified, *noAuthNoPriv* security level is assumed. If authentication is specified, select the hashing protocol to be used: HMAC authentication MD5 (by selecting **md5** in the command) or SHA (by selecting **sha** in the command), as well as the key-generating password.

NOTE The generation of the key is considerably slow. During the generation of the key the CLI will

stop responding for several seconds (depending on the switch model).

Users with security level *AuthNoPriv* and *AuthPriv* are stored in NVRAM when the **write** command is executed. The configured users will not be seen in the configuration file.

For a remote user, the ID of the remote SNMP engine must be specified.

Command Syntax

```
device-name(config)#snmp-server user USER-NAME group GROUP-NAME {v1 | v2c}

device-name(config)#snmp-server user USER-NAME group GROUP-NAME v3 [priv
ENCRYPTION] [auth {md5 | sha} PASSWORD] [remote ENGINE-ID]

device-name(config)#no snmp-server user USER-NAME [group GROUP-NAME {v1 |
v2c}]

device-name(config)#no snmp-server user USER-NAME group GROUP-NAME v3 [priv
ENCRYPTION] [auth {md5 | sha} PASSWORD] [remote ENGINE-ID]
```

Argument Description

USER-NAME	The name of the user on the host that connects to the agent. The user name is limited to 32 characters.
GROUP-NAME	The name of the group to which the user is associated.
v1, v2c, v3	Enter the SNMP version number (v1, v2c, or v3). If you enter v3, you have additional options.
priv ENCRYPTION	(Optional) Specifies that the PDUs sent from this user should be encrypted, with the key generated from the password.
auth	(Optional) An authentication level setting session. Specifying this argument requires either md5 or sha to be specified, as well as a password string.
md5	HMAC-MD5 authentication
sha	HMAC-SHA authentication
PASSWORD	The authentication password string (not to exceed 32 characters).
remote ENGINE-ID	(Optional) Creates a remote user by its engine-ID.

Example 1

The following example shows how to create a user named ***TOM*** that uses SNMP v1:

```
device-name(config)#snmp-server user TOM group g_all_v1 v1
```

Example 2

The following example shows how to create a user named ***TOM*** that uses SNMP v3 with authentication and privacy. The privacy password is ***privPass*** and the authentication password is ***authPass***:

```
device-name(config)# user TOM group g_all_v3 v3 priv privPass auth md5
authPass
```

Example 3

The following example shows how to remove a defined user named *IVAN* from an associated group ***ACC***:

```
device-name(config)#no snmp-server user IVAN group ACC v3
```

Configuring the SNMP Notification Log

The **snmp-server log-notify** command in Privileged (Enable) mode, enables the SNMP notification log. When used without arguments, the command enables logging of all notifications to the internal Flash memory. The **no** form of this command disables the SNMP notification log and clears its content.

Command Syntax

```
device-name#snmp-server log-notify [<Tag>]
device-name#no snmp-server log-notify [<Tag>]
```

Argument Description

Tag	Name of the tag associated with the notifications to be logged. If the parameter is not supplied, logging of all notifications is enabled/disabled.

NOTE

If logging of particular notifications has been disabled with a specific (with an argument) **no snmp-server log-notify** *Tag1* command, using the general (without the argument) **snmp-server log-notify** command will not enable them. In this case, you have to explicitly enable these notifications. E.g. if you have set

```
device-name#no snmp-server log-notify Tag1
```

then using

```
device-name#snmp-server log-notify
```

will enable all notifications except those associated with *Tag1*. To enable them, use

```
device-name#snmp-server log-notify Tag1
```

Clearing the SNMP Notification Log

The **clear snmp-server log-notify** command in Privileged (Enable) mode erases the content the SNMP notification log.

Command Syntax

```
device-name#clear snmp-server log-notify
```

Controlling the Access to the Switch

Table 10-2 lists the commands used for controlling the following access functions:

- Telnet access to the switch. For the use of named access list by telnet see "Configuring a Telnet Connection".
- Access of the SNMP users. For the use of named access list by SNMP see "SNMP Server Configuration".

Table 10-2 Access List Commands

Command	Description
access-list	Creates an access list that controls inbound and/or outbound data traffic according to specified criteria.
show access-lists	Displays the access lists of the routing protocols.

Default Access List Configuration

Table 10-3 shows the default parameters for the access list.

Table 10-3 Access List Default Configuration

Parameter	Default Value
Named access list	Not created
Exact match	Disabled

Creating a Named Access List

The **access-list** command, in Global Configuration mode, configures an access list that controls the inbound and/or outbound data traffic according to criteria specified in the command arguments. The **no** form of this command removes the specified access list.

The access list defaults to an implicit deny statement for any condition that has not been permitted.

Command Syntax

```
device-name(config)#access-list NAME {permit | deny} {A.B.C.D/M [exact-match]
| any}
device-name(config)#no access-list NAME [{permit | deny} {A.B.C.D/M }
```

Argument Description

NAME	The access list name (spaces are not allowed and the first character must be a letter).
permit	Permits access for matching conditions.
deny	Denies access to matching conditions.
A.B.C.D/M	Source IP address and mask.
any	Any IP address.

exact-match	Only the IPs with an exact match of the specified argument (used only for routing protocols).

Example

The following example shows a basic filtering configuration:

```
device-name(config)#access-list filter deny 10.0.0.0/9
device-name(config)#access-list filter permit 10.0.0.0/8
```

Displaying the Named Access Lists

The **show access-lists** command, in Privileged (Enable) mode, displays the defined named access lists.

Command Syntax

```
device-name#show access-lists
```

Example

The following example displays the defined rule for any routing protocol. The access list, named ***jiji***, permits access from any source. The access list, named ***phone***, permits all addresses from the range 34.34.34.6/16 that meet an exact match.

```
device-name(config)#access-list jiji permit any
device-name(config)#access-list phone permit 34.34.34.6/16
device-name#show access-lists
access-list jiji permit any
ccess-list phone permit 34.34.34.6/16
```

Assigning an Access List to a User

The **snmp-server access-list** command, in Global Configuration mode, assigns an access list to the specified user. The **no** form of this command, removes the access list assigned to the specified user.

The access list can permit or deny access to a user or according to the access list rule. The access list rules contain a **permit** or **deny** action and a source IP address. To define the named access list use the **access-list** command in Global Configuration mode. The defined access lists can be viewed by the **show access-lists** command in Privileged (Enable) mode.

Command Syntax

```
device-name(config)#snmp-server access-list USER-NAME ACL-NAME
device-name(config)#no snmp-server access-list USER-NAME
```

Argument Description

USER-NAME	The user name.
ACL-NAME	The access list name.

Example

```
device-name(config)#access-list MyLyst permit 220.132.0.0/16
device-name(config)#snmp-server access list UN MyLyst
```

Notification Configuration Commands

In order to send notifications to the management station, perform the following steps:

1. Enable the SNMP agent (if it is disabled).
2. Create a view, group and user that includes the notification variables with notify access right
3. Create a tag that includes all required notifications. See Defining SNMP Notification.
4. Create a target parameter that links a parameter name to the user. See Defining the Notification Target Parameter.
5. Create a target address that links the parameter to a specific IP address. See Defining the Notification Target Address.

Table 10-4 lists the configuration commands for the SNMPv3 Agent. By default, no notifications will be sent by the switch.

NOTE The user configured to receive the notification must have notify access (in the view) to all variables participating in the notification.

Table 10-4 Agent Notification Configuration Commands

Command	Description
snmp-server notify	Defines a notification and specifies the type (trap/inform).
snmp-server target-param	Defines the notification target parameter.
snmp-server target-addr	Defines the notification target address.
snmp-server target-profile	Includes or excludes a branch of the MIB tree in a notification profile.
snmp-server authentication-failure-trap	Enables sending authentication-failure traps globally.

Defining SNMP Notification

The **snmp-server notify** command, in Global Configuration mode, defines the notification. The **no** form of this command disables the notification.

NOTE The notification name is the same as specified in the MIB (case sensitive).

Command Syntax

```
device-name(config)#snmp-server notify NAME TAG-NAME
device-name(config)#no snmp-server notify NAME
```

Argument Description

NAME	The notification name, a reserved literal string. The available arguments are

	specified in Table 10-5.
TAG-NAME	The notification tag.

Example

```
device-name(config)#snmp-server notify linkUp tag1
```

Table 10-5 Notification Argument Values

Argument Value	Description
resilientLinkStatusChange	Indicates that the resilient link status was changed, identified by the resilientLinkIndex.
linkup	Indicates that the SNMP entity acting as an agent has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into another state (but not into the notPresent state). The other state is indicated by the included value of ifOperStatus.
linkDown	Indicates that the SNMP entity acting as an agent has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
coldStart	Indicates that the SNMP entity acting as an agent is reinitializing itself and that its configuration may have been altered.
warmStart	Indicates that the SNMP entity acting as an agent is reinitializing itself such that its configurationis unaltered.
authenticationFailure	Indicates that the SNMP entity acting as an agent has received a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP that is used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside of the authoritative SNMP engine's time window. Note: The generation of authentication failure notification is also controlled by the snmp-server authentication-failure-trap command.
risingAlarm	RMON alarm which is generated when a value rises above its pre-programmed threshold.
fallingAlarm	RMON alarm which is generated when a value falls below its pre-programmed threshold.
newRoot	Indicates that a new root is elected by the Spanning Tree algorithm.
portSecurityViolation	Indicates that a security violation was made on a port defined as a secure port. For more information, see

Argument Value	Description
topologyChange	Indicates that the topology change has been detected by the Spanning Tree algorithm.
unauthorizedAccessViaCLI	Indicates an attempt for unauthorized access via CLI. As unauthorized access is considered any occurrence of three consecutive wrong password entries when there are no users defined or any incorrect user name or password entry if there are users defined.
configurationLoadFailed	Indicates that download or upload of configuration file failed.
cpuUtilizationExceeded	Indicates that CPU utilization exceeded.
imageCrcCheckFailed	Indicates that download of OS image file failed in CRC check.
portRedundantLinkChange	Indicates that the link status of a redundant port has changed.
portsCRCErrExceeded	Indicates that level of CRC errors have passed the program threshold.
portsOverSizeExceeded	Indicates that level of oversize packets have passed the program threshold.
portsRuntsExceeded	Indicates that level of runts packets have passed the program threshold.
ramFreeSpaceExceed	Indicates that RAM space reaches critical minimum.
edtaskSuspended	Indicates that a task is suspended.

Defining the Notification Target Parameter

The **snmp-server target-param** command, in Global Configuration mode, defines the notification target parameter. The **no** form of this command removes the notification target parameter.

The SNMP server target parameter sets the trap security parameters and specifies the user that sends the trap to the target address. The target parameter defines the security level - *noAuthNoPriv*, *AuthNoPriv* or *AuthPriv*. The user data contains the keys for the trap PDU encryption. Optionally you can define a target-profile that represents a set of filters, which restrict the access to the MIB tree for trap sending.

Command Syntax

```
device-name(config)#snmp-server target-param NAME SEC-NAME v1|v2c [PROFILE]

device-name(config)#snmp-server target-param NAME SEC-NAME v3 {auth | |
noauth | priv} [PROFILE]

device-name(config)#no snmp-server target-param NAME
```

Argument Description

WORD	The name of the target parameter.
SEC-NAME	The security name.
v1, v2c, v3	The security model of the target-parameter. It specifies the version of the protocol in which the traps would be sent (**v1**, with TRAP-V1 PDU type or **v2c** and **v3**, with TRAP-V2 PDU type).
noauth	Security level, which implies no authentication and no encryption of the PDUs.
auth	Authentication of the PDUs based on HMAC-MD5 or HMAC-SHA. No encryption.
priv	Authentication based on HMAC-MD5 or HMAC-SHA and CBC-DES encryption for the message data.
PROFILE	(Optional) Profile name.

Example

```
device-name(config)#snmp-server target-param param1 ABC v3 auth
```

Defining the Notification Target Address

The **snmp-server target-addr** command, in Global Configuration mode, defines the notification target address. The **no** form of this command, deletes the notification target address.

Command Syntax

```
device-name(config)#snmp-server target-addr NAME A.B.C.D <udp-port> PAR-NAME
TAG1 [TAG2 ... TAGN]

device-name(config)#snmp-server target-addr NAME {addtag | deltag} TAG-NAME

device-name(config)#no snmp-server target-addr NAME
```

NOTE

The command with addtag and deltag arguments can be used only if the notification tag address was defined.

Argument Description

NAME	The name of the notification target address.
A.B.C.D	The IP address of the target.
udp-port	The UDP port number of the target address in the range <1-65535>.
PAR-NAME	Parameter name.
<TAG1> [<TAG2> ... <TAGN>]	A list of tags. You can add one or more tags.
addtag	Adds the specified tag to the list.
deltag	Removes the specified tag from the list.

TAG-NAME	The name of the added/removed tag.

Example 1

```
device-name(config)#snmp-server target-address XYZ 192.168.0.121 162 param1
tag1
```

Example 2

```
device-name(config)#snmp-server target-address XYZ addtag tag2
```

Enabling Sending Authentication Failure Traps

The **snmp-server authentication-failure-trap** command**,** in Global Configuration mode, enables sending authentication-failure traps. The **no** form of this command disables the authentication-failure trap.

This command controls the value of MIB-II mib-2.snmp.snmpEnableAuthenTraps.

Command Syntax

```
device-name(config)#snmp-server authentication-failure-trap
device-name(config)#no snmp-server authentication-failure-trap
```

Defining a Notification Target Profile

The **snmp-server target-profile** command, in Global Configuration mode, includes or excludes a branch of the MIB tree in a notification profile. The **no** form of this command removes the notification target profile. Use this command only if you need to supply filters that do not match the user definition.

In most cases the user can use the user defined filters by applying the **snmp-server user** command in Global Configuration mode.

NOTE Before you use this command, it is recommended that you read RFC 3413 section 6.

When you create target profiles, it is required that you include snmpTrapOID.0 in the profile.

Command Syntax

```
device-name(config)#snmp-server target-profile PROFILE-NAME OBJECT-ID
{included | excluded} [MASK]
device-name(config)#no snmp-server target-profile PROFILE-NAME OBJECT-ID
{included | excluded}
```

Argument Description

PROFILE-NAME	The name of the profile.
OBJECT-ID	The starting point inside the MIB tree given in dot-notation or as an object name.
included	The Object-ID is included in the profile.
excluded	The Object-ID is excluded from the profile.

MASK	(Optional) The bit-mask that defines Object ID wildcard characters.

SNMP MIB-II System Group Elements Commands

Table 10-6 lists the configuration commands for the SNMP MIB-II system group elements.

Table 10-6 SNMP MIB-II System Group Elements Configuration Commands

Command	Description
snmp-server contact	Sets the MIB-II system contact string.
snmp-server system-name	Sets the MIB-II system name.
snmp-server location	Sets the MIB-II system location string.

Defining the System Contact String

The **snmp-server contact** command, in Global Configuration mode, sets the MIB-II system contact string. The **no** form of this command removes the SNMP system contact string.

The system contact string is used for the textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is a zero-length string.

Command Syntax

```
device-name(config)#snmp-server contact .LINE-TEXT
device-name(config)#no snmp-server contact
```

Example

```
device-name(config)#snmp-server contact tom@comp.com
```

Argument Description

LINE-TEXT	Descriptive system contact string, up to 80 characters long.

Defining the System Name

The **snmp-server system-name** command, in Global Configuration mode, sets the MIB-II system name. The **no** form of this command removes the SNMP system name.

The system name is an administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is a zero-length string.

Command Syntax

```
device-name(config)#snmp-server system-name .LINE-TEXT
device-name(config)#no snmp-server system-name
```

Argument Description

.LINE-TEXT	System name, up to 80 characters long.

Example

```
device-name(config)#snmp-server system-name Nokia
```

Defining the System Location

The **snmp-server location** command, in Global Configuration mode, sets the MIB-II system location string. The **no** form of this command removes the SNMP system location string.

The system location string is used for describing the physical location of this node (e.g., "telephone closet", "3rd floor"). If the location is unknown, the value is a zero-length string.

Command Syntax

```
device-name(config)#snmp-server location .LINE-TEXT
device-name(config)#no snmp-server location
```

Argument Description

.LINE-TEXT	Descriptive system location string, up to 80 characters long.

Example

```
device-name(config)#snmp-server location ROOM 256
```

SNMP Displaying Commands

Table 10-7 lists the display commands for the SNMP Agent.

Table 10-7 SNMPv3 Agent Display Commands

Command	Description
show snmp-server	Displays the status of the SNMP server.
show snmp-server engineID	Displays the current SNMP agent engine ID and all remote Engine IDs that are known to the agent.
show snmp-server group	Displays all configured groups for the SNMP agent.
show snmp-server user	Displays all users and the local SNMP engine of the agent to which they are associated. Shows all the users defined for the SNMP agent
show snmp-server view	Displays all configured views for the SNMP agent.
show snmp-server target-param	Displays the target parameters.
show snmp-server target-profiles	Displays the notification target profiles.
show snmp-server notify	Displays information for the notify type (inform or trap).

Command	Description
show snmp-server target-addr	Displays the notification target address.
show snmp-server access-listshow snmp-server log-notify	Displays the access list assigned to a user.Displays the SNMP notification log.
show snmp-server informs	Display the pending informs.

Displaying the Status of the SNMP Server

The **show snmp-server** command, in Privileged (Enable) mode, displays the status of the SNMP server – enable or disable, and the UDP port on which the SNMP is enabled.

Command Syntax

```
device-name#show snmp-server
```

Example

```
device-name#show snmp-server

snmp-server enable
authentication-failure trap disable
Inform retries 10
Inform timeout 2 secs
device-name#
```

Displaying the Engine-ID

The **show snmp-server engineID** command, in Privileged (Enable) mode, displays the local SNMP engine ID of the SNMP agent, all Engine IDs that are known to the agent, and information about the Inform operation values that are different from their default values.

Command Syntax

```
device-name#show snmp-server engineID
```

Example

```
device-name#show snmp-server engineID

Local snmpEngineID: 000002DB0300A01211259A0000
snmpEngineBoots: 3, snmpEngineTime: 2394

Remote snmpEngineID: 80000523010A000001
snmpEngineBoots: 273, snmpEngineTime: 978
IP address: 10.0.0.1
device-name#
```

Displaying the SNMP Groups

The **show snmp-server group** command, in Privileged (Enable) mode, displays the configured groups, their associated views, and the security model. If the security model is USM (v3), the command displays the security level.

Command Syntax

```
device-name#show snmp-server group
```

Example

```
device-name#show snmp-server group
group name:     GR1             security model: v3  auth
read view:      READ            write view:     WRITE
notify view:    NOTIFY          row status:     active
device-name#
```

Displaying the SNMP Users

The **show snmp-server user** command, in Privileged (Enable) mode, displays the users and their associated engine ID.

Command Syntax

```
device-name#show snmp-server user
```

Example

```
device-name#show snmp-server user

User name: MAG
Engine ID:1234567890
Group: GR1 model:v3 Auth
device-name#
```

Displaying All Configured Views

The **show snmp-server view** command, in Privileged (Enable) mode, displays all configured views. This command displays the viewmask of a particular view if it is configured. If the name of the view is specified, only data for the views with the specified name is displayed on the screen. If the view name is not specified, all views are displayed on the screen. The view name is not case-sensitive and can be entered partially. The viewmask length is 32B.

A view is displayed in symbolic format, when some portions of the viewfamily OID match the OID, stored in file *batm_oid_table*. The symbol with the longest match of the OID is assigned and concatenated with the unmatched OIDs.

Command Syntax

```
device-name#show snmp-server view [VIEW-NAME]
```

Argument Description

VIEWNAME	(Optional) The name of the view. The view name is limited to 32 characters.

Example 1

The following example shows how to display a view family in symbolic format. The view family has the following long OID:

```
1.3.6.1.2.1.4.24.4.1.192.168.0.0.255.255.0.0.0.192.168.4.1
```

The view is displayed in the following format:

```
ipCidrRouteEntry.192.168.0.0.255.255.0.0.0.192.168.4.1
```

```
device-name#show snmp-server view

View name:   MyView
OID:         mib-2 included
Row status:  Active
Storage type:Volatile

View name:   MyView
OID:         sysUpTime excluded
Row status:  Active
Storage type:Volatile
device-name#
```

If the file *batm_oid_table* is loaded in the hidden directory of the flash file system, the OIDs will be shown with symbolic names.

The row status can be **Active** (the row is operable) or **notInService** (the row is administratively disabled).

The storage type can be **Volatile** (the data is in volatile memory, and after reboot it will be lost) or **Non Volatile** (the data is in Non volatile memory – it will be restored after reboot).

Displaying the Notification Target Parameters

The **show snmp-server target-param** command, in Privileged (Enable) mode, displays the notification target parameters.

Command Syntax

```
device-name#show snmp-server target-param
```

Example

```
device-name#show snmp-server target-param

Target Parameter: param1
Security Name: GHJ
Security Level: auth
Profile name: PROFILE
device-name#
```

Displaying the Notification Target Profiles

The **show snmp-server target-profiles** command, in Privileged (Enable) mode, displays the notification target profiles.

Command Syntax

```
device-name#show snmp-server target-profiles
```

Example

```
device-name#show snmp-server target-profiles
```

```
Profile name: profile
OID:          internet included

Profile name: profile
OID:          risingAlarm excluded
device-name#
```

Displaying the SNMP v2c/v3 Notification Type

The **show snmp-server notify** command, in Privileged (Enable) mode, displays the SNMPv2c and SNMPv3 notification parameters (name, type and tag). The notification type can be either "trap" or "inform request" ("inform" for short).

Command Syntax

```
device-name#show snmp-server notify
```

Example

```
device-name#show snmp-server notify

Notify Name: fanStatusChangelinkDown
Notify type: inform
Tag: tag1

Notify Name: linkUp
Notify type: inform
Tag: tag1

Notify Name: resilientLinkStatusChange
Notify type: trap
Tag: tag
device-name#
```

Displaying the Notification Target Address

The **show snmp-server target-addr** command, in Privileged (Enable) mode, displays the notification target address.

Command Syntax

```
device-name#show snmp-server target-addr
```

Example

```
device-name#show snmp-server target-addr

Target Address: YOU
IP address: 192.168.0.39
UDP port: 162
Target Parameter: param
Tag list: 1 tag1
device-name#
```

Displaying the Access List

The **show snmp-server access-list** command, in Privileged (Enable) mode, displays the access list applied to the server.

Command Syntax

```
device-name#show snmp-server access-list
```

Displaying the Pending Informs

The **show snmp-server informs** command, in Privileged (Enable) mode, displays the pending informs.

Command Syntax

```
device-name#show snmp-server informs
```

Example

```
device-name#show snmp-server informs
Number of pending informs :0
device-name#
```

Configuration Examples

Configuring SNMP v2c inform notifications:

1. Enable the SNMP server

```
device-name(config)#snmp-server enable
```

2. Define the notification with name NAME, tag TAG, and create the notification as an inform request:

```
device-name(config)#snmp-server notify NAME TAG inform
```

3. Define a notification target address with name ADDRESSNAME and IP address 193.124.13.6. Specify the default UDP port (162), the parameter name (PARAMNAME), and a tag (TAG).

```
device-name(config)#snmp-server target-addr ADDRESSNAME 193.124.13.6 162 PARAMNAME TAG
```

4. To configure SNMP V2c inform notification, define a notification target parameter with name PARAMNAME and security name *usrV2,* security model *v2.*

```
device-name(config)#snmp-server target-param PARAMNAME usrV2 v2c
```

5. Create a user with name *usrV2* and assign this user to group *grpV2*. Specify the SNMP version number *v2c*

```
device-name(config)#snmp-server user usrV2 group grpV2 v2c
```

6. Configure a group with name *grpV2*, SNMP version number *2.* Specify read view – *all.* Specify write view – *all*. Specify the notify view - *all*.

```
device-name(config)#snmp-server group grpV2 v2c read all write all notify all
```

7. Create a view with name all. Specify the OID-tree – Internet and include the Object ID in the view.

```
device-name(config)#snmp-server view all internet include
```

Configuring SNMP v3 inform notifications:

1. Enable the SNMP server:

```
device-name(config)#snmp-server enable
```

2. Define the notification with name *NAME,* tag *TAG* and create the notification as an inform:

```
device-name(config)#snmp-server notify NAME TAG inform
```

3. Define a notification target address with name *ADDRESSNAME* and IP address *193.124.13.6.* Specify the default UDP port (162), the parameter name (PARAMNAME), and a tag (TAG).

```
device-name(config)#snmp-server target-addr ADDRESSNAME 193.124.13.6 162 PARAMNAME TAG
```

4. Define a notification target parameter with name *PARAMNAME* and security name *usrRemote,* security model *v3* and Authentication of the PDUs based on HMAC-MD5 or HMAC-SHA.

```
device-name(config)#snmp-server target-param PARAMNAME usrRemote v3 auth
```

5. Create a user with name *usrRemote* and assign this user to group *grpRemote*. Specify the SNMP version number 3, authentication level auth with HMAC-SHA authentication, and authentication password string. Create a remote user with engine *ID 123456789abcd*.

```
device-name(config)#snmp-server user usrRemote group grpRemote v3 auth sha
auth_password remote 123456789abcd
```

6. Configure a group with name *grpRemote*, SNMP version number *3,* authentication level *auth.* Specify a read view – *all.* Specify a write view – *all*. Specify the notify view - *all*.

```
device-name(config)#snmp-server group grpRemote v3 auth read all write all notify all
```

7. Create a view with a name *all*. Specify the OID-TREE – *Internet* and include the Object ID in the view.

```
device-name(config)#snmp-server view all internet include
```

Displaying the SNMP Notification Log

The **show snmp-server log-notify** command, in Privileged (Enable) mode, displays the content of the SNMP notification log.

Command Syntax

```
device-name#show snmp-server log-notify [{first<1-65535> | last<1-65535>}]
```

Argument Description

first	(Optional) Displays the first <1-65535> records.
Last	(Optional) Displays the last <1-65535> records.

Example

```
device-name#show snmp-server log-notify
2004/01/15 12:38:06  linkUp notification sent: interface 1/1/5.
2004/01/15 12:38:05  linkDown notification sent: interface 1/1/5.
```

11. Forwarding Database (FDB)

Introduction

The MAC Address table contains the information that is in the forwarding database. The switch uses the forwarding database to forward packets to the appropriate bridge in the bridge group.

The FDB has both static entries, which are created by the user, and dynamic entries (learned entries), which are added and removed by the learning process. Static entries cannot be overwritten by the learning process, and are removed from the table only when you explicitly delete them.

MAC-Table Entry Types

There are several types of entries in the FDB (forwarding Database Table):

- **Dynamic entries** –Initially, all entries in the database are dynamic. Entries in the database are removed (aged-out) if, after a period of time (aging time), the device has not transmitted. If a device is removed from the network, its entry is deleted from the database. In this way, the database is not filled up with obsolete entries. If the switch is reset or a power Off/On cycle occurs, dynamic entries are deleted from the database. The dynamic entries can also be deleted by a specified command. More information about setting the aging time and deleting dynamic entries is provided further on in this section.
- **Static entries** – Static entries are configured by the user. These are permanent entries which are retained in the database if the switch is reset or a power off/on cycle occurs. The system administrator is responsible for making entries permanent. A permanent entry can be a unicast MAC address. All entries entered by way of the command-line interface are stored as permanent.
- **Secure entries** –A secure entry is configured to a secured port (configured by the **port security** command as described in the Port Security chapter), allowing only secured MAC addresses to be learned by this port.
- **Self entries –** A self entry is created automatically for each VLAN that is configured on the switch with the switch's MAC address.
- **Filtered entries** –Filtered entries are dynamic MAC addresses that perform security violation on secured port (configured by the **port security** command).

How Entries Are Added to the FDB

You can add entries into the FDB in the following two ways:

- The switch learns MAC addresses at the FDB with the following parameters: source MAC address, VLAN, interface and the VLAN priority (if any).
- You can add entry to the FDB statically.

Configuring and Displaying FDB Settings

Table 11-1 summarizes the commands for configuring and viewing FDB settings.

Table 11-1 FDB Configuration and Viewing Commands

Command	Description
mac-address-table	Adds an entry to the FDB table.
clear mac-address-table	Clears the specified MAC addresses.
no mac-address-table	Clears the specified MAC addresses.
show mac-address-table	Displays the specified data pertaining to the FDB table.
mac-address-table aging-time	Sets the FDB aging time.
show mac-address-table aging-time	Displays the FDB table aging time.

Description of Commands

Adding FDB Table Entries with the CLI

To add a new MAC address manually to the FDB table, use the following command in Configuration mode.

mac-address-table

The **mac-address-table** command, in Global Configuration mode, adds a static, dynamic or secure entry to the FDB table. The command specifies the entry's MAC address, the port number and the VLAN ID.

Command Syntax

```
device-name(config)#mac-address-table {static|dynamic|secure}
HH:HH:HH:HH:HH:HH interface UU/SS/PP vlan <vlan-id>
```

Argument Description

static	Add static entry.
dynamic	Add dynamic entry statically.
secure	Add secure entry for secured port (see Port Security).
HH:HH:HH:HH:HH:HH	48-bit hardware address
interface UU/SS/PP	The interface number
vlan <vlan-id>	The VLAN identifier in the range <1-4094>

Example

```
device-name(config)#mac-address-table static 00:0a:01:02:03:04 interface
1/1/1 vlan 2496
```

Deleting Entries

There are two types of commands to remove FDB entries:

- **clear mac-address-table** commands – applied in Privileged (Enable) mode;
- **no mac-address-table** commands – applied in Configuration mode.

The commands are implemented as follows:

clear mac-address-table

The **clear mac-address-table** command, in Privileged (Enable) mode, clears the MAC addresses specified by the command arguments.

Command Syntax

```
device-name#clear mac-address-table
[dynamic|filtered|secure|static|multicast][address HH:HH:HH:HH:HH:HH]
[vlan <vlan-id>] [interface UU/SS/PP]
```

Argument Description

address HH:HH:HH:HH:HH:HH	(Optional) The specified MAC address to be cleared, if it complies with all other specified arguments.
interface UU/SS/PP	(Optional) MAC addresses on the specified interface are cleared, if they comply with all other specified arguments.
vlan <vlan-id>	(Optional) MAC addresses for the specified VLAN are cleared, if they comply with all other specified arguments. The VLAN identifier in the range <1-4094>

dynamic	(Optional) Only dynamic MAC addresses are cleared.
filtered	(Optional) Only filtered MAC addresses are cleared.
secure	(Optional) Only secure MAC addresses are cleared.
static	(Optional) Only static MAC addresses are cleared.
multicast	(Optional) Only multicast MAC addresses are cleaned.

NOTE If any argument is omitted, the command clears all MAC addresses complying with the arguments that are specified.

no mac-address-table

The **no mac-address-table** command, in Global Configuration mode, clears the MAC addresses specified by the command arguments.

Command Syntax

```
device-name(config)#no mac-address-table
{dynamic|filtered|secure|multicast|aging-time} address HH:HH:HH:HH:HH:HH
[vlan <vlan-id>]

device-name(config)#no mac-address-table static address HH:HH:HH:HH:HH:HH
[vlan <vlan-id>] [interface UU/SS/PP]
```

Argument Description

address HH:HH:HH:HH:HH:HH	The specified MAC address is cleared, if it complies with all other specified arguments.
interface UU/SS/PP	(Optional) MAC addresses on the specified interface are cleared, if they comply with all other specified arguments.
vlan <vlan-id>	(Optional) MAC addresses for the specified VLAN are cleared, if they comply with all other specified arguments. The VLAN identifier is in the range <1-4094>
dynamic	Only dynamic MAC addresses are cleared.
filtered	Only filtered MAC addresses are cleared.
secure	Only secure MAC addresses are cleared.
static	Only static MAC addresses are cleared.
multicast	Only multicast MAC addresses are cleared.
aging-time	set default MAC address table aging-time

Displaying FDB Table Entries

show mac-address-table

The **show mac-address-table** command, in Privileged (Enable) mode, displays the FDB entries stored in the switch, and other data pertaining to the FDB table, as specified by the command arguments.

Command Syntax

```
device-name#show mac-address-table [dynamic|filtered|secure|static] [address
HH:HH:HH:HH:HH:HH] [vlan <vlan-id>] [interface UU/SS/PP]

device-name#show mac-address-table count
```

Argument Description

address HH:HH:HH:HH:HH:HH	(Optional) Information is displayed about the specified MAC address, if it complies with all other specified arguments.
interface UU/SS/PP	(Optional) Information is displayed about the MAC addresses on the specified interface, if they comply with all other specified arguments.
vlan <vlan-id>	(Optional) Information is displayed about the MAC addresses for the specified VLAN, if they comply with all other specified arguments.
dynamic	(Optional) Information is displayed only about the dynamic MAC addresses.
filtered	(Optional) Information is displayed only about the filtered MAC addresses.
secure	(Optional) Information is displayed only about the secure MAC addresses.
static	(Optional) Information is displayed only about the static MAC addresses.
count	Displays the number of entries in the FDB table.
aging-time	Display MAC address table aging-time
multicast	Display multicast addresses
self	Display self addresses

NOTE If no arguments are specified, the show mac-address-table command displays the entire FDB table.

Example

The following command displays the entire FDB table.

```
device-name#show mac-address-table

====+========+====================+==========+=================+==========|
  # |   VID  |  Mac               |  PORT    |  STATUS         | PRIORITY |
----+--------+--------------------+----------+-----------------+----------+
  1 |  0001  |  00:00:00:00:11:22 |  1/1/3   |  static         | 0        |
  2 |  0001  |  00:40:95:30:0e:8f |  1/1/7   |  dynamic        | 0        |
```

```
  3 |  0001  |  00:a0:12:05:36:80  |          |  self          | 0        |
```

Setting the MAC Address Aging Time

The MAC address aging time is the time interval that a dynamic MAC address is allowed to remain on the FDB table without sending any frame to the device. If the aging time expires, the address of the network is removed from the FDB table. The following command sets the MAC address aging time.

mac-address-table aging-time

The **mac-address-table aging-time** command, in Global Configuration mode, sets the MAC address aging time value. The **no** form of this command turns the aging-time counter off. The default aging-time value is 300 seconds.

NOTE The actual aging time may take up to twice as long as the value that has been set, e.g. if 300 seconds have been specified, the actual age-out period may take between 300 and 600 seconds.

Command Syntax

```
device-name(config)#mac-address-table aging-time <TIME>
device-name(config)#no mac-address-table aging-time
```

Argument Description

TIME	The aging time value in seconds, in the range <10-816>

Example

The following example sets the MAC Address aging time to 800 seconds (13.3 minutes):

```
device-name(config)#mac-address-table aging-time 800
```

show mac-address-table aging-time

The **show mac-address-table aging-time** command, in Privileged (Enable) mode, displays the MAC address aging time.

Command Syntax

```
device-name(config)#show mac-address-table aging-time
```

Example

The following example shows how to display the currently configured aging time:

```
device-name(config)#show mac-address-table aging-time
aging time is 1500 seconds
```

12. Spanning Tree Protocol (STP)

Introduction

The Spanning Tree Algorithm and Protocol are part of the ANSI/IEEE Std 802.1D MAC Bridges specifications sponsored by the LAN/MAN Standards Committee of the IEEE Computer Society.

STP (Spanning-Tree Protocol) provides fault tolerance on networks, by allowing you to implement parallel paths for network traffic. The algorithm creates a spanning tree (a loop-free subset of the network topology), that enables a learning bridge to dynamically work around loops in a network topology. STP allows you to implement redundant paths that are enabled only when the main paths fail.

STP configuration is disabled by default.

Configuring and Debugging STP

You can use STP configuration commands per switch or per interface. To enable per-switch STP configuration commands, you must enter Protocol Configuration mode, by using the following command in global Configuration mode:

```
device-name(config)#protocol
device-name(cfg protocol)#
```

The `(cfg protocol)#` prompt-line indicates Protocol Configuration mode.

To access the STP interface configuration commands, use the following command in global Configuration mode:

```
device-name(config)#interface UU/SS/PP
device-name(config-if UU/SS/PP)#
```

Argument Description

UU/SS/PP	Unit, slot and port number of an interface (i.e. – 1/1/8).

The `(config-if UU/SS/PP)#` prompt-line indicates interface ***UU/SS/PP*** Configuration mode.

Table 12-1 summarizes the STP commands available in Protocol Configuration mode.

Table 12-2 summarizes the STP commands available in interface configuration mode.

Table 12-3 summarizes the STP debug commands.

Table 12-1 STP Commands in Protocol Configuration Mode

Command	Description
spanning-tree	Displays the current STP parameter settings.
spanning-tree enable/disable	Enables/disables the STP option.
spanning-tree priority	Sets the STP bridge priority
spanning-tree hello-time	Sets time interval between BPDU transmissions from the ports of this unit
spanning-tree forward-delay	Sets the time duration in Listening and Learning states that precede the Forwarding state. Also used to age dynamic entries in the Forwarding database when a topology change is under way.
spanning-tree max-age	Sets the time that learned STP information is kept before being discarded.
spanning-tree interface	Changes to specified interface configuration mode and displays the STP settings for that interface.
spanning-treeline-error-detect	Reconfigures the STP or RSTPto use the alternate (backup) link in case of CRC errors.

NOTE A BPDU (Bridge Protocol Data Unit) transmission is an STP information-exchange packet sent out at periodic intervals to other units in the network, to detect loops in the network topology.

Table 12-2 STP Commands in Interface Configuration Mode

Command	Description
spanning-tree all	Displays all STP ports table
spanning-tree path-cost	Sets STP port path-cost
spanning-tree priority	Sets STP port priority
spanning-tree defaults	Sets the STP parameters to their default values for the configured interface.
spanning-tree detect-tc	Enables Topology change detection.

Table 12-3 STP Debug Commands

Command	Description
debug stp	Displays the STP debug messages as specified by the command argument.
show debug stp	Displays the status of the STP debug actions that are currently activated.

STP Configuration Commands in Protocol Configuration Mode

spanning-tree

The **spanning-tree** command, in Protocol Configuration mode, displays the current STP parameter configuration. To display Spanning-Tree topology for a specified port or all ports, use the **show spanning-tree interface** command or the **show spanning-tree** command in Privileged mode.

Command Syntax

```
device-name(cfg protocol)#spanning-tree
```

Example

```
device-name(cfg protocol)#spanning-tree
Spanning tree              enabled
ProtocolSpecification   = ieee8021d
Priority                = 32768
TimeSinceTopologyChange = 18364 (sec)
TopChanges              = 107
DesignatedRoot          = 32768.00:A0:12:0F:18:4D
RootCost                = 19
RootPort                = 1/1/1
MaxAge                  = 20 (sec)
HelloTime               = 1  (sec)
HoldTime                = 1  (sec)
BridgeMaxAge            = 20 (sec)
BridgeHelloTime         = 1  (sec)
BridgeForwardDelay      = 15 (sec)
DetectLineCRCReconfig   = disabled
```

spanning-tree enable/disable

The **spanning-tree enable/disable** command, in Protocol Configuration mode, enables/disables the Spanning Tree option.

The Spanning Tree algorithm dynamically creates a tree through the network used to efficiently direct packets to their destinations. When STP is enabled, the unit acts as a node in the tree. When STP is disabled, you can still use the other commands to set the STP configuration. These settings are preserved when STP is enabled. To disable the spanning tree you can also use the **no** form of the command.

By default, STP is disabled.

Command Syntax

```
device-name(cfg protocol)#spanning-tree {enable|disable}
device-name(cfg protocol)#no spanning-tree
```

Argument Description

enable	Enables the Spanning Tree.
disable	Disables the Spanning Tree.

spanning-tree priority

The **spanning-tree priority** command, in Protocol Configuration mode, assigns the specified value to the STP bridge priority. The default value is 32768. The **no** form of this command resets the default value.

Command Syntax

```
device-name(cfg protocol)#spanning-tree priority <0-65535>
device-name(cfg protocol)#no spanning-tree priority
```

Argument Description

0- 65535	The spanning tree bridge priority. The default value is 32768.

spanning-tree hello-time

The **spanning-tree hello-time** command, in Protocol Configuration mode, sets the time interval in seconds between BPDU transmissions from the ports of this unit. You use this command when the unit is the root of the Spanning Tree, or trying to become so. The default value is 2 seconds and the range depends on the MaxAge value (between 1 and 10 seconds). The **no** form of this command resets the default value.

NOTE  You cannot assign hello-time a value greater than MaxAge/2-1.

Command Syntax

```
device-name(cfg protocol)#spanning-tree hello-time <hello-time>
device-name(cfg protocol)#no spanning-tree hello-time
```

Argument Description

hello-time	The time interval in seconds between BPDU transmissions from the ports of this unit. The default value is 2 seconds.

spanning-tree forward-delay

The **spanning-tree forward-delay** command, in Protocol Configuration mode, sets the time, in seconds, that the switch stays in each of the Listening and Learning states that precede the Forwarding State. In addition, when a topology change is underway and has been detected, this parameter is used to age all dynamic entries in the Forwarding database. The default value is 15 seconds, and the range depends on the MaxAge value (between 4 and 30 seconds). The **no** form of this command resets the default value.

NOTE  You cannot assign forward-delay a value less than MaxAge/2+1.

Command Syntax

```
device-name(cfg protocol)#spanning-tree forward-delay <forward-delay>
```

```
device-name(cfg protocol)#no spanning-tree forward-delay
```

Argument Description

forward-delay	The time in seconds that the switch stays in each of the Listening and Learning states that precede the Forwarding State. The default value is 15 seconds.

spanning-tree max-age

The **spanning-tree max-age** command, in Protocol Configuration mode, sets the time in seconds that learned Spanning Tree information is kept before being discarded. The default value is 20 second, and the range depends on the hello time and forward delay values (between 4 and 30 seconds). The **no** form of this command resets the default value.

NOTE You cannot assign MaxAge a value that is less than 2*(hello-time + 1) or more than 2*(forward-delay – 1).

Command Syntax

```
device-name(cfg protocol)#spanning-tree max-age <max-age>
device-name(cfg protocol)#no spanning-tree max-age
```

Argument Description

max-age	The time in seconds during which learned Spanning Tree information is maintained before being discarded. The default value is 20 seconds.

spanning-tree interface

The **spanning-tree interface** command, in Protocol Configuration mode, changes the mode to the specified interface Configuration mode and enables the setting of the STP in the specified interface, if a specific interface is specified. If **all** is specified, this command displays the Spanning-Tree topology for all ports (the configuration mode stays the same). The command is equivalent to the **spanning-tree all** command in any logical interface configuration mode. See also Displaying Port Spanning-Tree Topology Settings**.**

Command Syntax

```
device-name(cfg protocol)#spanning-tree interface {UU/SS/PP|all}
```

Argument Description

UU/SS/PP	Unit, slot and Port number of interface to be configured. The configuration mode is changed accordingly.
all	The configuration mode does not change. Spanning Tree topology for all ports is displayed.

Examples

1. Setting the spanning-tree priority of interface 1/1/1 to 100:

```
device-name(cfg protocol)#spanning-tree interface 1/1/1
```

```
PortPriority       = 128
PortState          = disabled
PortEnable         = disabled
PortPathCost       = 10
DesignatedRoot     = 08192.00:A0:12:00:00:03
DesignatedCost     = 19
DesignatedBridge   = 32768.00:A0:12:11:29:82
DesignatedPort     = 128.1
FrwrdTransitions   = 0
TopChangeDetection = Enabled
device-name(config-if 1/1/1)#spanning-tree priority 100
```

2. Displaying the spanning-tree topology for all interfaces:

```
device-name(cfg protocol)#spanning-tree interface all
================================================================================
===
Port    |Pri|State|PCost| Cost  |Designated bridge |DPrt  |FwrdT|DtctTc
--------+---+-----+-----+-------+------------------+------+-----+--------
01/01/01 128 listn    19     19  32768.00A012000003 128.01    2 Disabled
01/01/02 128 block    19      0  32768.000002030405 128.63    0 Enabled
01/01/03 128 listn    19      0  32768.000002030405 128.62    2 Enabled

device-name(cfg protocol)#
```

spanning-tree line-error-detect

The **spanning-tree line-error-detect enable** command, in Protocol Configuration mode, switches the device to using the existing alternate (backup) link instead of the current link, when the CRC errors on the line reach critical level. The error level is considered critical when the CRC error rate exceeds 1% for a 3-seconds interval. The command triggers reconfiguring of the Spanning Tree or the Rapid Spanning Tree, so it is effective only when either STP or RSTP is enabled.

The **spanning-tree line-error-detect disable** command disables detecting of CRC errors.

Command Syntax

```
device-name(cfg protocol)#spanning-tree line-error-detect {enable|disable}
```

Argument Description

enable	Enables detecting of CRC errors and STP/RSTP reconfiguring.
disable	Disables detecting of CRC errors.

STP Configuration Commands in Interface Configuration Mode

spanning-tree all

The **spanning-tree all** command, in Interface Configuration mode, displays the current status of spanning-tree parameters for all the switch's logical interfaces. The command is equivalent

to the **spanning-tree interface all** command in Protocol Configuration mode. See also Displaying Port Spanning-Tree Topology Settings.

Command Syntax

```
device-name(config-if UU/SS/PP)#spanning-tree all
```

Example

```
device-name(config-if 1/1/1)#spanning-tree all
================================================================================
Port    |Pri|State|PCost |   DCost   |Designated bridge |DPrt  |FwrdT|DtctTc
--------+---+-----+------+-----------+------------------+------+-----+------
--
01/01/01 128 listn    19      19       32768.00A012000003 128.01  2 Disabled
01/01/17 128 block    19       0       32768.000002030405 128.63  0 Enabled
01/01/19 128 listn    19       0       32768.000002030405 128.62  2 Enabled
```

spanning-tree path-cost

The **spanning-tree path-cost** command, in Interface Configuration mode, sets the STP port path-cost for the configured interface. The **no** form of this command resets the default path-cost value of 10.

Command Syntax

```
device-name(config-if UU/SS/PP)#spanning-tree path-cost <1-200000000>
device-name(config-if UU/SS/PP)#no spanning-tree path-cost
```

Argument Description

<1-200000000>	STP path-cost value assigned to the configured interface.

spanning-tree priority

The **spanning-tree priority** command, in Interface Configuration mode, sets the STP priority for the configured interface. The **no** form of this command resets the default priority value of 128.

Command Syntax

```
device-name(config-if UU/SS/PP)#spanning-tree priority <0-255>
device-name(config-if UU/SS/PP)#no spanning-tree priority
```

Argument Description

<0-255>	STP priority value assigned to the configured interface.

spanning-tree defaults

The **spanning-tree defaults** command, in Interface Configuration mode, restores the STP parameters to their defaults for the configured interface.

Command Syntax

```
device-name(config-if UU/SS/PP)#spanning-tree defaults
```

NOTE This command replaces the no spanning-tree command in Interface Configuration mode.

spanning-tree detect-tc

The **spanning-tree detect-tc** command, in Interface Configuration mode, enables topology change detection on the configured interface. Use the **no** form of the command to disable the topology change detection.

The ability to detect topology changes can be enabled or disabled on a per-Port basis by the **spanning-tree detect-tc** command. The intent of this facility is to allow topology change detection to be disabled on Ports where it is known that a single end station is connected, and where powering that end station on and off would cause the Topology Change Notification mechanism to be triggered.

By default, the topology change detection is enabled.

Command Syntax

```
device-name(config-if UU/SS/PP)#spanning-tree detect-tc
device-name(config-if UU/SS/PP)#no spanning-tree detect-tc
```

Displaying Port Spanning-Tree Topology Settings

Table 12-4 STP Display Commands in View / Privileged Mode

Command	Description
show spanning-tree	Displays the current STP parameter settings, and Spanning-Tree topology of all ports.
show spanning-tree interface	Displays the Spanning-Tree topology for the specified port.

show spanning-tree

The **show spanning-tree** command, in Privileged (Enable) mode, displays the current STP parameters settings and Spanning-Tree topology for all ports.

Command Syntax

```
device-name#show spanning-tree
```

Example

When the bridge is not the root bridge:

```
device-name#show spanning-tree
Spanning tree              enabled
ProtocolSpecification   = ieee8021d
Priority                = 32768
TimeSinceTopologyChange = 60 (sec)
TopChanges              = 4
DesignatedRoot          = 08192.00:A0:12:00:00:03
RootPort                = 01/01/15
RootCost                = 19
MaxAge                  = 6  (sec)
HelloTime               = 1  (sec)
ForwardDelay            = 4  (sec)
HoldTime                = 1  (sec)
BridgeMaxAge            = 20 (sec)
BridgeHelloTime         = 2  (sec)
BridgeForwardDelay      = 15 (sec)
DetectLineCRCReconfig   = disabled

Port    |Pri|State|PCost |    DCost    |Designated bridge |DPrt
|FwrdT|DtctTc
--------+---+-----+------+-------------+------------------+------+-----+----
01/01/01 128 listn    19       19       32768.00A012000003 128.01     2
Disabled
01/01/02 128 block    19       0        32768.000002030405 128.63     0
Enabled
01/01/03 128 listn    19       0        32768.000002030405 128.62     2
Enabled
```

show spanning-tree interface

The **show spanning-tree interface** command, in Privileged (Enable) mode, displays the Spanning-Tree topology for the specified port.

Command Syntax

```
device-name#show spanning-tree interface UU/SS/PP
```

Example

The following example displays the STP interface parameters when the bridge is not the Root Bridge:

```
device-name#show spanning-tree interface 1/1/1
PortPriority       = 128
PortState          = disabled
PortEnable         = disabled
PortPathCost       = 10
DesignatedRoot     = 08192.00:A0:12:00:00:03
DesignatedCost     = 19
DesignatedBridge   = 32768.00:A0:12:11:29:82
DesignatedPort     = 128.1
FrwrdTransitions   = 0
TopChangeDetection = Enabled
```

The following example displays the STP interface parameters when the bridge is the Root Bridge:

```
device-name#show spanning-tree interface 1/1/1
```

```
PortPriority       = 128
PortState          = disabled
PortEnable         = disabled
PortPathCost       = 10
DesignatedRoot     = This bridge is the root
DesignatedCost     = 0
DesignatedBridge   = This bridge
DesignatedPort     = 128.1
FrwrdTransitions   = 0
TopChangeDetection = Enabled
```

Debugging STP

Table 12-5 lists the STP debugging commands.

Table 12-5 STP Debugging Commands

Command	Description
debug stp	Displays the information related to processing the Spanning Tree Protocol (STP).
show debug stp	Displays the debug status for the Spanning Tree protocol (STP).

Enabling STP Debug Information

The **debug stp** command, in Privileged (Enable) mode, displays the information related to processing the Spanning Tree protocol (STP). Use the **no** form of this command to disable the display of STP information.

The STP debug commands will not be saved after reload.

By default, the debug is disabled.

Command Syntax

```
device-name#debug stp {all|flush|tc|tcn}
device-name#no debug stp {all|flush|tc|tcn}
```

Argument Description

all	Activates all STP debug options.
flush	Activates MAC address table flush debugging.
tc	Activates debugging when the switch receives or transmits BPDU with topology change.
tcn	Activates debugging when the switch receives TCN or transmits BPDU with topology change ACK.

Displaying the Status of the STP Debug

The **show debug stp** command, in Privileged (Enable) mode, displays the debug status for the Spanning Tree protocol (STP). The debug commands can help the network manager to monitor a session as it proceeds on the switch.

Command Syntax

```
device-name#show debug stp
```

13. Rapid Spanning Tree Protocol (RSTP)

Introduction

RSTP (Rapid Spanning Tree Protocol) performs the roles of the STP protocol considerably faster by enabling rapid transitions of ports from Alternate state to Root state, and from Backup state to *Designated* state. In certain cases, RSTP enables rapid transitions of ports to Forwarding states.

RSTP is based on IEEE Std 802.1W and is part of *Amendment 2: Rapid Reconfiguration* to IEEE Std 802.1D and IEEE Std 802.1t-2001.

RSTP assigns to each bridge port throughout the Bridged Local Area Network one of the roles summarized in Table 13-1.

Table 13-1 RSTP Port Role Assignments

Port Role	Definition
Root Port	Port connected to the root bridge/switch. State: forwarding and link enabled.
Designated Port	Port connected to the designated switch - the switch closest to the root switch. Frames are forwarded to the root through the designated switch.
Alternate Port	Port that offers a path to the root bridge/switch alternate to the path provided by the Root Port. The Alternate Port can replace the current root port if link failure or a configuration change such as port priority change occurs. State: discarding and link enabled.
Backup Port	Backup for the path provided by a Designated Port in the direction of the leaves of the Spanning Tree. Points away from the root. State: discarding and link enabled.
Disabled Port	Blocked port. State: discarding and link disabled.

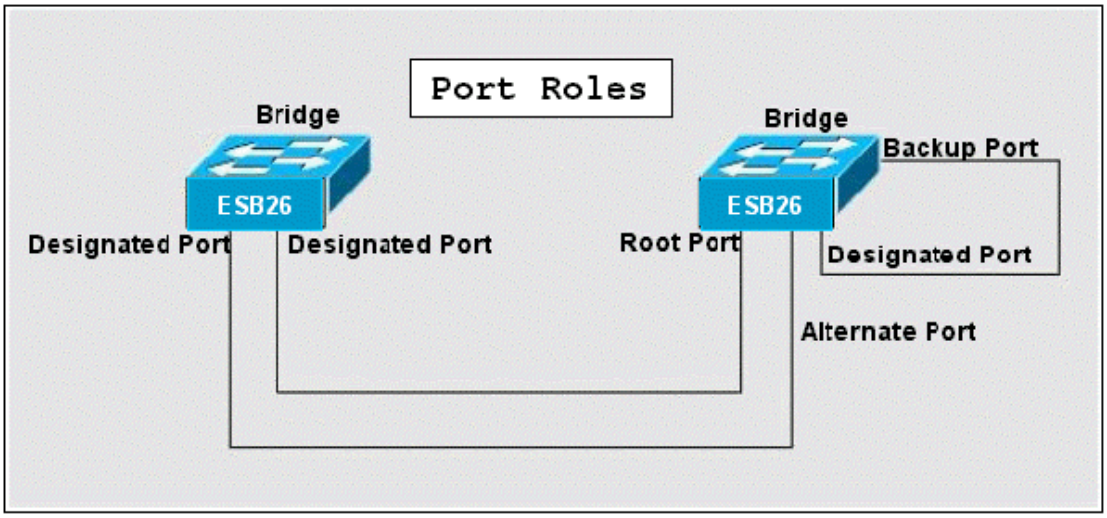


Figure 13-1 RSTP Port Roles

The RSTP port roles are determined automatically by the following parameters:

- a unique Bridge Identifier associated to each bridge;
- a Path Cost associated to each bridge port;
- a unique Port Identifier associated to each bridge port.

Selection of the Root Bridge and Root Port

RSTP automatically selects the bridge that has the best **Bridge Identifier** as the **Root Bridge**. Each bridge has a unique Bridge Identifier that is derived from the Bridge Address and from a manageable priority component (described in **IEEE Std 802.1w-2001, Part 3: Media Access Control (MAC) Bridges, Amendment 2: Rapid Reconfiguration, Section 9.2.5: *Encoding of Bridge Identifiers*).** The unique Bridge Identifiers are compared numerically, assigning the highest priority to the lowest identifier value (the best Bridge Identifier).

A Root **Path Cost** is associated with every Bridge, by summing up the path costs for each Bridge Port receiving frames on the least cost path from the Root Bridge to that Bridge. The path cost associated with the Root Bridge this is zero. The Path Cost associated with all other ports may be manageable.

For each bridge except for the Root Bridge, RSTP automatically assigns the role of **Root Port** to the Bridge Port that receives frames on the least cost path from the Root Bridge. If two or more ports on a bridge have the same least Path Cost sum from the Root, then RSTP selects the port that has the best **Port Identifier** as the Root Port.

The **Port Identifier** comprises two parts. One part is fixed and unique for each Port on a Bridge. The other part is a manageable priority component (as described in **IEEE Std 802.1w-2001, Part 3: Media Access Control (MAC) Bridges, Amendment 2: Rapid Reconfiguration, Section 9.2.7**: ***Encoding of Port Identifiers***). The unique Port Identifiers are compared numerically, assigning the highest priority to the lowest identifier value (the best Port Identifier).

Selection of the Designated Bridge and Designated Port

RSTP associates a Root **Path Cost** to every LAN in the Bridged Local Area Network. This is the Root Path Cost of the lowest cost Bridge with a Bridge Port connected to that LAN. RSTP selects this Bridge as the **Designated Bridge** for that LAN. If two or more Bridges have the same Root Path Cost, then the Bridge with the best priority (least numerical value) is selected as the Designated Bridge. The Bridge Port on the Designated Bridge that is connected to the LAN is assigned the role of **Designated Port** for that LAN. If the Designated Bridge has two or more ports connected to the LAN, then the Bridge Port with the best priority Port Identifier (least numerical value) is selected as the Designated Port.

In a Bridged LAN with a stable physical topology (i.e., the information communicated by the RST Algorithm is consistent throughout the network), each LAN has one single Designated Port, and each Bridge except for the Root Bridge has a Root Port connected to a LAN. Any operational Bridge Port that is not assigned a role of Root Port or Designated Port is either of the following:

- a Backup Port - if the Bridge is the Designated Bridge for the attached LAN

OR OTHERWISE

- an Alternate Port.

Alternate and Backup Ports

An Alternate Port offers a path in the direction of the Root Bridge alternate to that provided by the Bridge's Root Port.

A Backup Port acts as a backup for the path provided by a Designated Port in the direction of the leaves of the Spanning Tree. Backup Ports exist only where a given Bridge has two or more connections to a given LAN, Therefore, backup ports (and the Designated Ports that they back up) can exist only where two ports are connected together in loopback by a point to point link, or where the Bridge has two or more connections to a shared media LAN segment.

The distinction between the Alternate and Backup Port Roles was introduced in RSTP in order to describe the possibility of the rapid transition of an Alternate port to forwarding if the Root Port fails.

Point-To-Point Links

Some of the rapid state transitions that are possible within RSTP depend on whether the Port concerned can be connected to only one other Bridge (i.e., it is served by a point-to-point LAN segment), or to two or more Bridges (i.e., it is served by a shared medium LAN segment).

Rapid transition of a Designated Port to Forwarding is possible only if the LAN segment associated with the Port is point-to-point, or if the port is defined to be an edge Port. Otherwise, the transition of a Designated Port from Discarding to Learning and from learning to Forwarding occurs with a delay of Forward Delay.

Changing Port States

The Port States are controlled by a state machine, designed to maximize connectivity without introducing temporary data loops in the network. The state machine attempts to transition Root Ports and Designated Ports to the Forwarding Port State, and Alternate Ports and Backup Ports to the Discarding Port State, as rapidly as possible.

Transitions to the Discarding Port State can be simply effected without the risk of data loops. Transition of a Port to the Forwarding Port State needs to be consistent with the Port Roles assigned to other Ports in the region of the network.

A Bridge knows that the transition to the Forwarding Port State can be made if:

1. The Port Role has been Root Port or Designated Port long enough FOR:

   spanning Tree information supporting this role assignment to have reached all Bridges in the network,

   AND FOR

contradictory information to be received from any Bridge following the change in Spanning Tree information that first caused this Port to be assigned the Root Port or Designated Port role.

OR

2. The Port is now a Root Port AND:

   any Ports on the Bridge that have been Root Port too recently for Spanning Tree information to have definitely reached all Bridges in the network

   OR

   any Ports have been contradicted if necessary, are not and will not be put in the Forwarding Port State until that time has elapsed (with the exception of 3. below).

   OR

3. The Port is:

   a Designated Port and attaches to a LAN that has at most one other Bridge attached

   AND

   the other Bridge's Port Role assignments are consistent with this port's Bridge

   AND

   both Port States are known not to be Forwarding if they attach to LANs that connect to Bridges whose Port Roles are not consistent with that Bridge.

   OR

4. The Port is a Designated Port, attached to a LAN that is known not to be attached to any other Bridge Ports.

Condition 1 above makes use of Forwarding Delay as the basis for establishing that enough time has elapsed to allow the transition to the Forwarding state.

Configuring and Debugging RSTP

You can use RSTP configuration commands per switch or per interface.

To enable per-switch RSTP configuration commands, you must enter Protocol Configuration mode, by using the following command in global Configuration mode:

```
device-name(config)#protocol
device-name(cfg protocol)#
```

The (cfg protocol)# prompt-line indicates Protocol Configuration mode.

To access the RSTP interface configuration commands, use the following command in global Configuration mode:

```
device-name(config)#interface UU/SS/PP
device-name(config-if UU/SS/PP)#
```

Argument Description

UU/SS/PP	Unit, slot and port number of an interface (i.e. – 1/1/8).

The (config-if *UU/SS/PP*)# prompt-line indicates interface ***UU/SS/PP*** Configuration mode.

Table 13-2 summarizes the RSTP commands available in Protocol Configuration mode.

Table 13-3 summarizes the RSTP commands available in interface configuration mode.

Table 13-4 summarizes the RSTP debug commands.

Table 13-2 RSTP Commands in Protocol Configuration Mode

Command	Description
rapid-spanning-tree	Displays the current RSTP parameter settings.
rapid-spanning-tree enable/disable	Enables/disables the RSTP option.
rapid-spanning-tree priority	Sets the RSTP bridge priority
rapid-spanning-tree hello-time	Sets time interval between BPDU transmissions from the ports of this unit, in hundredths of seconds.
rapid-spanning-tree forward-delay	Sets the time duration in Listening and Learning states that precede the Forwarding state, in hundredths of seconds. Also used to age dynamic entries in the Forwarding database when a topology change is under way.
rapid-spanning-tree max-age	Sets the time, in seconds, that learned RSTP information is kept before being discarded.
rapid-spanning-tree interface	Changes to specified interface configuration mode and displays the RSTP settings for that interface.

NOTE A BPDU (Bridge Protocol Data Unit) transmission is an RSTP information-exchange packet sent out at periodic intervals to other units in the network, to detect loops in the network topology.

Table 13-3 RSTP Commands in Interface Configuration Mode

Command	Description
rapid-spanning-tree all	Displays all RSTP ports table
rapid-spanning-tree edge-port	Determines if the configured interface is an edge port.
rapid-spanning-tree link-type	Sets the RSTP port link type.
rapid-spanning-tree path-cost	Sets RSTP port path-cost
rapid-spanning-tree priority	Sets RSTP port priority

rapid-spanning-tree defaults	Sets the RSTP parameters to their defaults for the configured interface.
rapid-spanning-tree detect protocols	Recalculates the protocol migration state.
rapid-spanning-tree point_to_point_mac	Set RSTP port point_to_point_mac.

Table 13-4 RSTP Debug Commands

Command	Description
debug rstp	Displays the RSTP debug messages as specified by the command argument.
show debug rstp	Displays the status of the RSTP debug actions that are currently activated.

RSTP Configuration Commands in Protocol Configuration Mode

rapid-spanning-tree

The **rapid-spanning-tree** command, in Protocol Configuration mode, displays the current RSTP parameter configuration. To display Rapid-Spanning-Tree topology for a specified port or all ports, use the **show rapid-spanning-tree** command or the **show rapid-spanning-tree interface** command in View or Privileged mode.

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree
```

Example

```
device-name(cfg protocol)#rapid-spanning-tree
Rapid spanning tree     = enabled
ProtocolSpecification   = ieee8021w
Priority                = 32768
TimeSinceTopologyChange = 102 (Sec)
TopChanges              = 4
DesignatedRoot          = 04096.00:A0:12:00:00:03
RootPort                = 01/01/03
RootCost                = 200000
MaxAge                  = 20 (Sec)
HelloTime               = 2  (Sec)
ForwardDelay            = 15 (Sec)
BridgeMaxAge            = 20 (Sec)
BridgeHelloTime         = 3  (Sec)
BridgeForwardDelay      = 11 (Sec)
TxHoldCount             = 3
MigrationTimer          = 3  (Sec)
DetectLineCRCReconfig   = disabled
```

rapid-spanning-tree enable/disable

The **rapid-spanning-tree enable/disable** command, in Protocol Configuration mode, enables/disables the Rapid-Spanning Tree option.

When RSTP is disabled, you can still use the other commands to set the RSTP configuration. These settings are preserved when RSTP is enabled.

By default, RSTP is disabled.

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree {enable|disable}
```

Argument Description

enable	Enable the spanning tree status.
disable	Disable the spanning tree status.

rapid-spanning-tree priority

The **rapid-spanning-tree priority** command, in Protocol Configuration mode, assigns the specified value to the RSTP bridge priority. The **no** form of this command resets the default value 32768.

If the command is issued without specifying the priority value, it will display the currently configured priority value.

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree priority <0-65535>
device-name(cfg protocol)#no rapid-spanning-tree priority
```

Argument Description

0-65535	The rapid spanning tree bridge priority in increments of 4096. Any other number will be rounded down. The default value is 32768 (IEEE802.1w).

rapid-spanning-tree hello-time

The **rapid-spanning-tree hello-time** command, in Protocol Configuration mode, sets the time interval, in seconds, between BPDU transmissions from the ports of this unit. You use this command when the unit is the root of the Rapid Spanning Tree, or trying to become so. The default value is 2 seconds and the range depends on the MaxAge value (between 1 and 10 seconds). The **no** form of this command resets this time interval to its default value.

NOTE You cannot assign `hello-time` a value greater than `MaxAge`/2-1.

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree hello-time <hello-time>
device-name(cfg protocol)#no rapid-spanning-tree hello-time
```

Argument Description

hello-time	The time interval, in seconds, between BPDU transmissions from the ports of this unit. The default value is 2 seconds.

rapid-spanning-tree forward-delay

The **rapid-spanning-tree forward-delay** command, in Protocol Configuration mode, sets the time, in seconds, that the switch stays in each of the Listening and Learning states that precede the Forwarding State. In addition, when a topology change is underway and has been detected, this parameter is used to age all dynamic entries in the Forwarding database. The default value is 15 seconds, and the range is depends on the MaxAge value (between 4 and 30 seconds). The **no** form of this command resets to the default value.

NOTE  You cannot assign forward-delay a value less than MaxAge/2+1.

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree forward-delay <forward-delay>
device-name(cfg protocol)#no rapid-spanning-tree forward-delay
```

Argument Description

forward-delay	The time, in seconds, that the switch stays in each of the Listening and Learning states that precede the Forwarding State. The default value is 15 seconds.

rapid-spanning-tree max-age

The **rapid-spanning-tree max-age** command, in Protocol Configuration mode, sets the time in seconds that learned Rapid Spanning Tree information is kept before being discarded. The default value is 20 seconds, and the range depends on the hello-time and forward- delay values (between 4 and 30 seconds. The **no** form of this command resets to the default value.

NOTE  You cannot assign MaxAge a value that is less than 2*(hello-time + 1) or more than 2*(forward-delay – 1).

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree max-age <6-28>
device-name(cfg protocol)#no rapid-spanning-tree max-age
```

Argument Description

6-28	The time, in seconds, during which learned Spanning Tree information is kept before being discarded. The default value is 20 seconds.

rapid-spanning-tree interface

The **rapid-spanning-tree interface** command, in Protocol Configuration mode, changes the mode to interface configuration mode. This mode enables you to set the RSTP interface configuration. If the argument **all** is specified, this command displays the Rapid-Spanning-Tree topology for all ports and does not change the configuration mode. See also Displaying Port Rapid-Spanning-Tree Topology Settings**.**

Command Syntax

```
device-name(cfg protocol)#rapid-spanning-tree interface {UU/SS/PP|all}
```

Argument Description

UU/SS/PP	Unit, slot and port number of interface to be configured. The configuration mode is changed accordingly.
all	The configuration mode does not change. Rapid Spanning Tree topology for all ports is displayed.

Examples

1. The following examples display the output of the RSTP interface for an interface with link enabled:

```
device-name(cfg protocol)#rapid-spanning-tree interface 1/1/1
PortPriority          = 128
PortState             = forwarding
PortRole              = Designated Port
PortEnable              = enabled
PortPathCost          = 200000
DesignatedRoot        = This bridge is the root
DesignatedCost        = 0
DesignatedRoot        = This bridge
DesignatedPort        = 128.62
FrwrdTransitions      = 1
Admin EdgePort        = disabled
EdgePort              = disabled
AdminLink-Type        = Auto
Link-Type             = P2P
MigrationTimer        = 3
```

2. The following example displays the rapid-spanning-tree topology for all interfaces:

```
device-name(cfg protocol)#rapid-spanning-tree interface all
================================================================================
Port    |Pri|State|PCost   |DCost   |Designated
bridge|Prt|FwrdT|DtctTc
--------+---+-----+--------+--------+-----------------+-----+-----+-
--
01/01/01 128 listn 19       19 32768.00A012000003 128.01    2
Disabled
01/01/02 128 block 19        0 32768.000002030405 128.63    0 Enabled
01/01/03 128 listn 19        0 32768.000002030405 128.62    2 Enabled
```

RSTP Configuration Commands in Interface Configuration Mode

rapid-spanning-tree all

The **rapid-spanning-tree all** command, in Interface Configuration mode, displays the current status of rapid-spanning-tree parameters for all the switch's logical interfaces. The command is equivalent to the **rapid-spanning-tree interface all** command in Protocol Configuration mode. See also Displaying Port Rapid-Spanning-Tree Topology Settings.

Command Syntax

```
device-name(config-if UU/SS/PP)#rapid-spanning-tree all
```

Example

```
device-name(config-if 1/1/1)#rapid-spanning-tree all
================================================================================
Port   |Pri|State|PCost |DCost |Designated bridge |   DPrt   |FwrdT|DtctTc
-------+---+-----+------+------+------------------+--------+-----+--------
01/01/01128 listn 19     19     32768.00A012000003  128.01     2   Disabled
01/01/02128 block 19      0     32768.000002030405  128.63     0   Enabled
01/01/03128 listn 19      0     32768.000002030405  128.62     2   Enabled
```

rapid-spanning-tree edge-port

The **rapid-spanning-tree edge-port** command, in Interface Configuration mode, changes the admin status. The **no** form of this command disables the admin status.

The *EdgePort* parameter is controlled by the RSTP state machine and the Command Line Interface (CLI):

Admin EdgePort

The admin *EdgePort* parameter can be set by the CLI on a per-Port basis in order to indicate that a given Port is permitted to transit directly to the Forwarding Port State when a Port becomes *Designated*.

This functionality is provided in order to permit Bridge Ports that are (administratively) known to be at the edge of the Bridged LAN to transition to Forwarding without delay.

However, as the presence of a Bridge on a Port that has been marked as an edge Port could potentially cause a loop in the active topology, it is necessary to qualify the value of the administrative state variable according to the port's knowledge of whether or not any BPDUs have been received on the Port.

EdgePort

The Bridge Detection state machine controls the value of the corresponding operational state variable, operational EdgePort, which may be used in order to determine whether a port that becomes *Designated* is permitted to transit directly to Forwarding. A value of *enabled* in the show commands indicates that this state transition

is permitted to occur.

If a BPDU is received on the Port, then the value of operational EdgePort is set to *disabled*. Following a port initialization, or following a link-up event, operational EdgePort is set to the value of admin EdgePort.

Hence, if a Port that has been marked as an edge-port proves not to be one (due to the presence of another Bridge), then it will cease to behave like an edge-port until such a time as it is reinitialized (either by a link up/down event or by reissuing the CLI command).

NOTES

1. If a BPDU is received on a port defined as an edge port, it automatically reverts to edge-port disabled status. After link up/down the port returns to the admin status.
2. This command replaces the rapid-spanning-tree operEdge {0|1} command which will be supported only in upgrading versions.

Command Syntax

```
device-name(config-if UU/SS/PP)#rapid-spanning-tree edge-port
device-name(config-if UU/SS/PP)#no rapid-spanning-tree edge-port
```

rapid-spanning-tree link-type

The **rapid-spanning-tree link-type** command, in Interface Configuration mode, sets the RSTP port **link-type** administrative of the port. The **no** form of the command resets the link type to its default value (auto).

There are two statuses of link state: operational and administrative.

1. Admin Link-Type:

Auto

From the point of view of determining the value of the link-type, the switch is considered to be connected to a point-to-point LAN segment if any of the following conditions are true:

The ESB26 switch supports autonegotiation, and the autonegotiation function has determined that the LAN segment is to be operated in full duplex mode.

The switch entity has been configured by management means for full duplex operation. Otherwise, the MAC is considered to be connected to a LAN segment that is not point-to-point (shared media).

Point-to-point

Switch is considered to be connected to a point-to-point LAN segment which forces the operational link-type to be point-to-point.

Shared

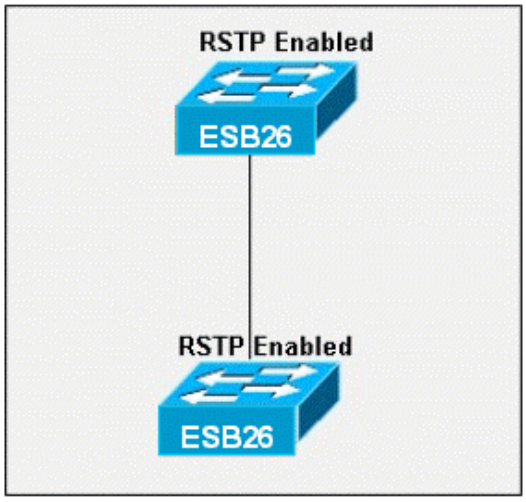
Switch is considered to be connected to a shared media LAN segment which forces the operational link-type to be *Shared*.

2. Operational link-type

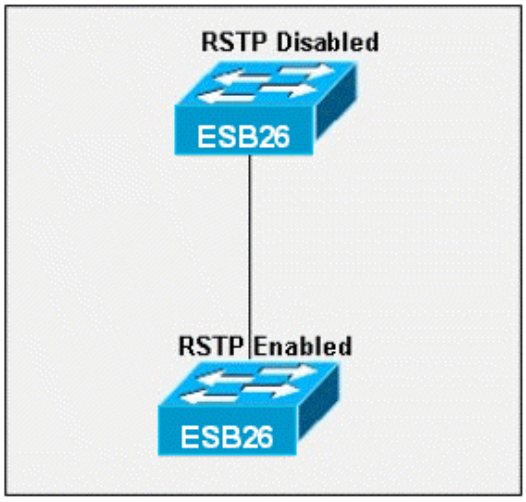
If Admin link-type is set to Auto, then the value of Operational link-type is determined in accordance with the specific procedures defined for the switch entity concerned, as defined in Admin link-type (auto).

If these procedures determine that the switch entity is connected to a point-to-point LAN segment, then Operational link-type is set to point-to-point, otherwise it is set to *Shared*.

In the absence of a specific definition of how to determine whether the switch is connected to a point-to-point LAN segment or not, the value of link-type shall be *Shared*.



point-to-point mac



NOT a point-to-point mac

Command Syntax

```
device-name(config-if UU/SS/PP)#rapid-spanning-tree link-type {auto|point-
to-point|shared}
device-name(config-if UU/SS/PP)#no rapid-spanning-tree link-type
```

Argument Description

auto	Indicates that the link type status is chosen dynamically according to the link state.
point-to-point	Indicates that the configured interface is connected to one switch, which runs RSTP. In point to point rapid, transition to Forwarding state is allowed in certain cases.
shared	Indicates that the interface is not connected to a single switch that is running RSTP.

rapid-spanning-tree path-cost

The **rapid-spanning-tree path-cost** command, in Interface Configuration mode, sets the RSTP port path-cost for the configured interface. The **no** form of this command resets the default path-cost (see table 13-1).

Command Syntax

```
device-name(config-if UU/SS/PP)#rapid-spanning-tree path-cost <1-200000000>
```

```
device-name(config-if UU/SS/PP)#no rapid-spanning-tree path-cost
```

Argument Description

1-200000000	RSTP path-cost value assigned to the configured interface.

Table 13-5 displays the default value that calculated from the link speed of the interface.

Table 13-5 Default Path cost values (IEEE8021w)

Link Speed	Recommended Value	Recommended Range	Valid Range
<=100 Kbps	200,000,000	20,000,000-200,000,000	1-200,000,000
1 Mbps	20,000,000	2,000,000-20,000,000	1-200,000,000
10 Mbps	2,000,000	200,000-2,000,000	1-200,000,000
100 Mbps	200,000	20,000-200,000	1-200,000,000
1 Gbps	20,000	2,000-200,000	1-200,000,000
10 Gbps	2,000	200-20,000	1-200,000,000
100 Gbps	200	20-2,000	1-200,000,000
1 Tbps	20	2-200	1-200,000,000
10 Tbps	2	1-20	1-200,000,000

rapid-spanning-tree priority

The **rapid-spanning-tree priority** command, in Interface Configuration mode, sets the RSTP priority for the configured interface. The **no** form of this command resets the default priority value of 128.

Command Syntax

```
device-name(config-if 1/1/1)#rapid-spanning-tree priority <0-255>
device-name(config-if 1/1/1)#no rapid-spanning-tree priority
```

Argument Description

0-255	RSTP priority value assigned to the configured interface in increments of 16. Any other number will be rounded down. The default value is 128 (IEEE802.1w).

rapid-spanning-tree defaults

The **rapid-spanning-tree defaults** command, in Interface Configuration mode, restores the RSTP parameters to their defaults for the configured interface.

Command Syntax

```
device-name(config-if 1/1/1)#rapid-spanning-tree defaults
```

rapid-spanning-tree detect-protocols

The **rapid-spanning-tree detect-protocols** command, in Interface Configuration mode, forces the port to work by the Rapid Spanning Tree Protocol (RSTP) and not by the Spanning Tree Protocol (STP).

A switch running RSTP supports a built-in protocol migration mechanism that enables RSTP to interoperate with legacy 802.1D STP.

When an RSTP switch receives a legacy 802.1D configuration BPDU (BPDU with protocol version 0) it start transmitting legacy 802.1D BPDU (configuration messages and TCN messages), however, when the switch stops receiving BPDU it cannot automatically revert to the RSTP mode because the switch cannot determine whether the legacy switch has been removed from that link unless the legacy switch is a designated switch

The RSTP supports a mechanism that forces the port to restart protocol migration process (force the renegotiation with neighboring switches) by mean of:

1. CLI command **rapid-spanning-tree detect-protocols.**

2. A link up event.

Command Syntax

```
device-name(config-if 1/1/1)#rapid-spanning-tree detect-protocols
```

Displaying Port Rapid-Spanning-Tree Topology Settings

Table 13-6 RSTP Display Commands in View / Privileged Mode

Command	Description
show rapid-spanning-tree	Displays the current RSTP parameter settings, and Rapid-Spanning-Tree topology of all ports.
show rapid-spanning-tree interface	Displays the Rapid-Spanning-Tree topology for the specified port.

show rapid-spanning-tree

The **show rapid-spanning-tree** command, in Privileged (Enable) mode, displays the current RSTP parameter settings and Rapid-Spanning-Tree topology for all ports.

Command Syntax

```
device-name#show rapid-spanning-tree
```

Example

```
device-name#show rapid-spanning-tree

Rapid spanning tree     = enabled

ProtocolSpecification   = ieee8021w

Priority                = 32768

TimeSinceTopologyChange = 32 (Sec)
TopChanges               = 3
DesignatedRoot          = 04096.00:A0:12:00:00:03
RootPort                = 01/01/03
RootCost                = 200000
MaxAge                  = 20 (Sec)
HelloTime               = 2  (Sec)
ForwardDelay            = 15 (Sec)
BridgeMaxAge            = 20 (Sec)
BridgeHelloTime         = 2  (Sec)
BridgeForwardDelay      = 15 (Sec)
TxHoldCount             = 3
MigrationTimer          = 3  (Sec)
DetectLineCRCReconfig   = disabled


================================================================================
Port   |Pri|Prt role|State|PCost |DCost |Designated bridge |DPrt  |FwrdT
-------+---+--------+-----+------+------+------------------+------+-----
01/01/03 128 Root   frwrd  200000 0     04096.00A012000003  128.31   1
01/01/04 128 Altern discr  200000 0     04096.00A012000003  128.37   1
```

show rapid-spanning-tree interface

The **show rapid-spanning-tree interface** command, in Privileged (Enable) mode, displays the Rapid-Spanning-Tree topology for the specified port.

Command Syntax

```
device-name#show rapid-spanning-tree interface UU/SS/PP
```

Example

In the following example the DesignatedRoot value indicates that the bridge is the root.

```
device-name#show rapid-spanning-tree interface 1/1/1
PortPriority         = 128
PortState        = forwarding
PortRole         = Designated Port
PortEnable       = enabled
```

```
PortPathCost        = 200000
DesignatedRoot      = This bridge is the root
DesignatedCost      = 0
DesignatedRoot      = This bridge
DesignatedPort      = 128.62
FrwrdTransitions    = 1
Admin EdgePort      = disabled
EdgePort            = disabled
AdminLink-Type      = Auto
Link-Type           = P2P
MigrationTimer      = 3
```

Debugging RSTP

Table 13-7 lists the RSTP debugging commands.

Table 13-7 RSTP Debugging Commands

Command	Description
debug rstp	Displays the information related to processing the Rapid Spanning Tree protocol (RSTP).
show debug rstp	Displays the status of Rapid Spanning Tree protocol (RSTP) debugging.

Enabling RSTP Debug Information

The **debug rstp** command, in Privileged (Enable) mode, displays the information related to processing the Rapid Spanning Tree protocol (RSTP). Use the **no** form of this command to disable the display of RSTP information.

The RSTP debug commands will not be saved after reload.

An example of the debug output after link failure is:

```
tSpanRecv: 1970/01/01 04:11:03 : link down on port 1/2/4


0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Select-Port-Roles
0xa1391880 (tSpanPRS):
=================
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Port 1/2/1 Is DesignatedPort
0xa1391880 (tSpanPRS):
```

```
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): End-Roles-Selection



tSpanRecv: 1970/01/01 04:11:06 : link up on port 1/2/4


0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Select-Port-Roles
0xa1391880 (tSpanPRS):
=================
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Port 1/2/1 Is DesignatedPort
0xa1391880 (tSpanPRS): Port 1/2/4 Is DesignatedPort
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): End-Roles-Selection



0xa139eb20 (tSpanPRT): Designated synced port 1/2/4
0xa139eb20 (tSpanPRT): Designated proposing port 1/2/4
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Select-Port-Roles
0xa1391880 (tSpanPRS):
=================
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Port 1/2/1 Is DesignatedPort
0xa1391880 (tSpanPRS): Port 1/2/4 Is DesignatedPort
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): End-Roles-Selection



0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Select-Port-Roles
0xa1391880 (tSpanPRS):
=================
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): Port 1/2/1 Is DesignatedPort
0xa1391880 (tSpanPRS): Port 1/2/4 Is BackupPort
0xa1391880 (tSpanPRS):
```

```
0xa1391880 (tSpanPRS):
0xa1391880 (tSpanPRS): End-Roles-Selection


By default, the debug is disabled.
```

Command Syntax

```
device-name#debug rstp {all | handshake | roles | flush}
device-name#no debug rstp {all | handshake | roles | flush}
```

Argument Description

all	Activates all RSTP debug options.
handshake	Activates Hand Shake protocol debugging (IEEE 802.1w).
roles	Activates debugging of role selection (designated port, root port, etc.)
flush	Activates debugging of port table flushing (MAC addresses).

Displaying the Status of the RSTP Debug

The **show debug rstp** command, in Privileged (Enable) mode, displays the status of Rapid Spanning Tree protocol (RSTP) debugging. The debug commands can help the network manager to monitor a session as it proceeds on the switch.

Command Syntax

```
device-name#show debug rstp
```

14. Multiple Spanning Tree Protocol (MSTP)

Introduction

The Multiple Spanning Tree (MST) protocol carries the concept of the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) a leap forward by allowing you to group and associate VLANs to multiple spanning tree instances (forwarding paths) over Link Aggregation Groups (LAGs). Used in a VLAN environment, this added capability affords rapid convergence as well as load balancing.

Each Multiple Spanning Tree Instance (MSTI) can have its own independent topology. The multiplicity of forwarding paths provided by this architecture improves network fault tolerance, because if one instance fails, data flow continues unaffected over the remaining forwarding paths. You can manage large networks and use redundant paths more easily by allocating different VLAN and spanning tree instance assignments in different parts of the network.

NOTE Terms used in this section are defined in Table 14-1.

Bridges running MST provide interoperability with Single Spanning Tree (SST) bridges, as follows:

- MST bridges run Internal Spanning Tree (IST). IST adds internal information about the MST region to the Common Spanning Tree (CST) information.
- IST connects all the MST bridges in the region and appears as a sub-tree in the CST that includes the whole bridged domain.
- Adjacent single Spanning Tree (SST) and MST regions regard the MST region as a single virtual bridge.
- The Common and Internal Spanning Tree (CIST) is the collection of the following:
    - Internal Spanning Trees (ISTs) in each MST region;
    - The Common Spanning Tree (CST) that interconnects the MST regions;
    - The SST bridges.

    Within an MST region, CIST is identical to an IST.

    Outside an MST region, CIST is identical to a CST.

    The STP, RSTP, and MSTP together elect a single bridge as the root of the CIST.

Within each MST region, MST establishes and maintains MST instances (MSTIs). These are additional spanning trees calculated by MSTP to provide a simply and fully connected active

topology for frames classified as belonging to VLANs that are mapped to the MSTI by the MST Configuration Table used by the MST Bridges of each MST Region. The IST is numbered 0, and the MSTIs are numbered 1, 2, 3, and so on. Each MSTI is local to the MST region and is independent of MSTIs in the other regions, even if the MST regions are interconnected.

Feature Overview

Definitions and Acronyms

Table 14-1 defines terms that are used in this document and lists their acronyms as specified in the IEEE 802.1s standard.

Table 14-1 Definitions and Acronyms of Terms

Term	Acronym	Definition
Boundary Port	--	A Bridge Port attaching an MST Bridge to a LAN that is in another region.
Common Spanning Tree	CST	The single Spanning Tree calculated by STP and RSTP, and by MSTP to connect MST Regions.
Common and Internal Spanning Tree	CIST	A collection of the ISTs in each MST region, and the common spanning tree (CST) that interconnects the MST regions. The CIST is calculated by MSTP to ensure that all LANs in the Bridged Local Area Network are simply and fully connected.
Internal Spanning Tree	IST	The connectivity provided by the CIST within a given MST Region. The IST is the first MSTI in the region, numbered as MSTI0, and it exists by default and cannot be removed. All other MST instances are numbered from 1 to 15.
Multiple Spanning Tree Instance	MSTI	One of a number of Spanning Trees calculated by MSTP within an MST Region. The MSTI is defined per VLAN group, and is designed to provide a simply and fully connected active topology for frames classified as belonging to VLANs that are mapped to the MSTI by the MST Configuration Table that is used by the MST Bridges of that MST Region.
MST Configuration Table	--	A configurable table that allocates each and every possible VLAN to the Common Spanning Tree or a specific Multiple Spanning Tree Instance.
MST Bridge	--	A Bridge capable of supporting the CST, and one or more MSTIs, and of selectively mapping frames classified in any given VLAN to the CST or a given MSTI.
MST Configuration Identifier	MCID	A name for, revision level, and a summary of a given allocation of VLANs to Spanning Trees. NOTE—Each MST Bridge uses a single MST Configuration Table and Configuration Identifier.

Term	Acronym	Definition
MST Region	--	A set of LANs and MST Bridges physically connected via Ports on those MST Bridges, where each LAN's CIST Designated Bridge is an MST Bridge, and each Port is either the Designated Port on one of the LANs, or else a non-Designated Port of an MST Bridge that is connected to one of the LANs, whose MCID matches exactly the MCID of the Designated Bridge of that LAN. NOTE—It follows from this definition that the MCID is the same for all LANs and Ports in the Region, and that the set of MST Bridges in the region are interconnected by the LANs.
Single Spanning Tree Bridge	SST Bridge	A Bridge capable of supporting only a single spanning tree, the CST. The single spanning tree may be supported by the Spanning Tree Algorithm and Protocol (STP) or by the Rapid Spanning Tree Algorithm and Protocol (RSTP).

Multiple Spanning-Tree Regions

To enable switches to participate in multiple spanning-tree instances (MSTIs), you must consistently configure the switches with the same MST configuration information. A collection of interconnected switches that have the same MST configuration comprises an MST region except for the case where the switches are connected through a shared media (i.e., LAN).

The MST configuration determines to which MST region each switch belongs. The configuration includes the name of the region, the revision number, and the MST instance-to-VLAN assignment map.

A region can have one member or multiple members with the same MST configuration. Each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

IST, CIST, and CST

Table 14-1 describes the conventional terms and acronyms used in MSTP.

The MSTP establishes and maintains two types of spanning-trees:

- **IST** - An internal spanning tree, which is the spanning tree that runs in an MST region. Within each MST region, the MSTP maintains multiple spanning-tree instances. Instance 0 is a special instance for a region, known as the internal spanning tree (IST). All other MST instances are numbered from 1 to 15.

  The IST is the only spanning-tree instance that sends and receives BPDUs. All other spanning-tree instance information is contained in M-records, which are encapsulated within MSTP BPDUs. Because the MSTP BPDU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced. All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth. By default, all VLANs are assigned to the IST. An MST instance is local to the region; for example, MST instance 1 in region A is

independent of MST instance 1 in region B, even if regions A and B are interconnected.

- **CIST** - A common and internal spanning tree, which is a collection of the ISTs in each MST region, and the common spanning tree (CST) that interconnects the MST regions and single spanning trees. The spanning tree calculated in a region appears as a subtree in the CST that encompasses the entire switched domain. The CIST is formed as a result of the spanning-tree algorithm running between switches that support the 802.1W, 802.1S, and 802.1D protocols. The CIST inside an MST region is the same as the CST outside a region.

Operations within an MST Region

The IST connects all the MSTP switches in a region. When the IST converges, the root of the IST becomes the IST master (shown in Figure 14-1), which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master is also the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP switches at the boundary of the region is selected as the IST master.

When an MSTP switch initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The switch also initializes all of its MST instances and claims to be the root for all of them. If the switch receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

During initialization, a region might have many subregions, each with its own IST master. As switches receive superior IST information, they leave their old subregions and join the new subregion that might contain the true IST master. Thus all subregions shrink, except for the one that contains the true IST master. For correct operation, all switches in the MST region must agree on the same IST master. Therefore, any two switches in the region synchronize their port roles for an MST instance only if they converge to a common IST master.

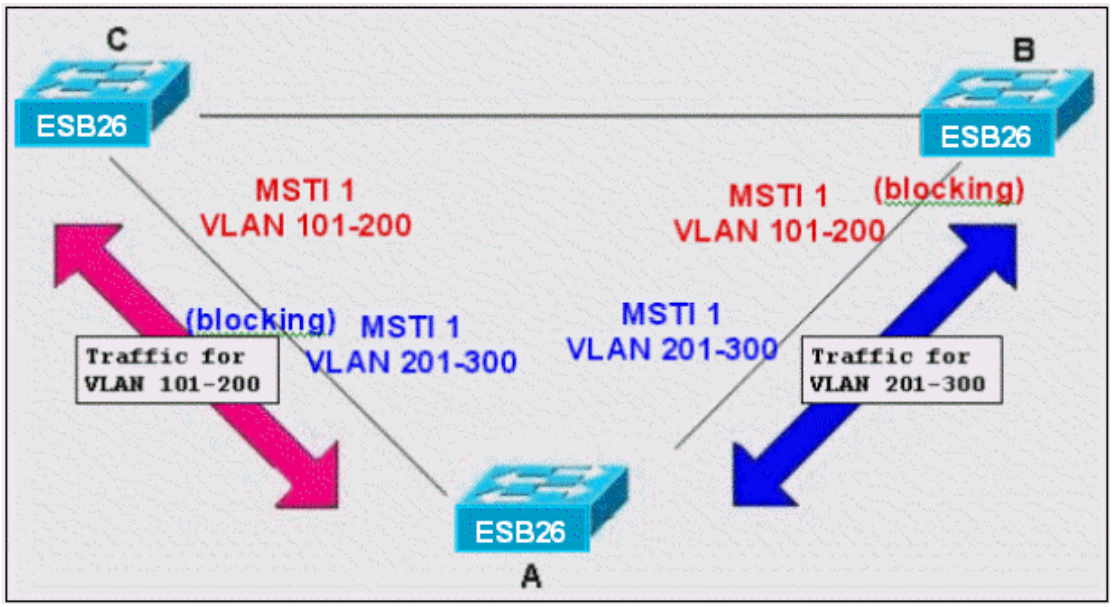


Figure 14-1 MSTP Within a Region

Operation between MSTP Regions

If there are multiple regions or legacy 802.1D switches within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP switches in the

network. The MST instances combine with the IST at the boundary of the region to become the CST. The IST connects all the MSTP switches in the region and appears as a subtree in the CST that encompasses the entire switched domain, with the root of the subtree being the IST master. The MST region appears as a virtual switch to adjacent STP switches and MST regions. Figure 14-2 shows a network with three MST regions and a legacy 802.1D switch (D). The IST master for region 1 (A) is also the CST root. The IST master for region 2 (B) and the IST master for region 3 (C) are the roots for their respective subtrees within the CST. The RSTP runs in all regions.

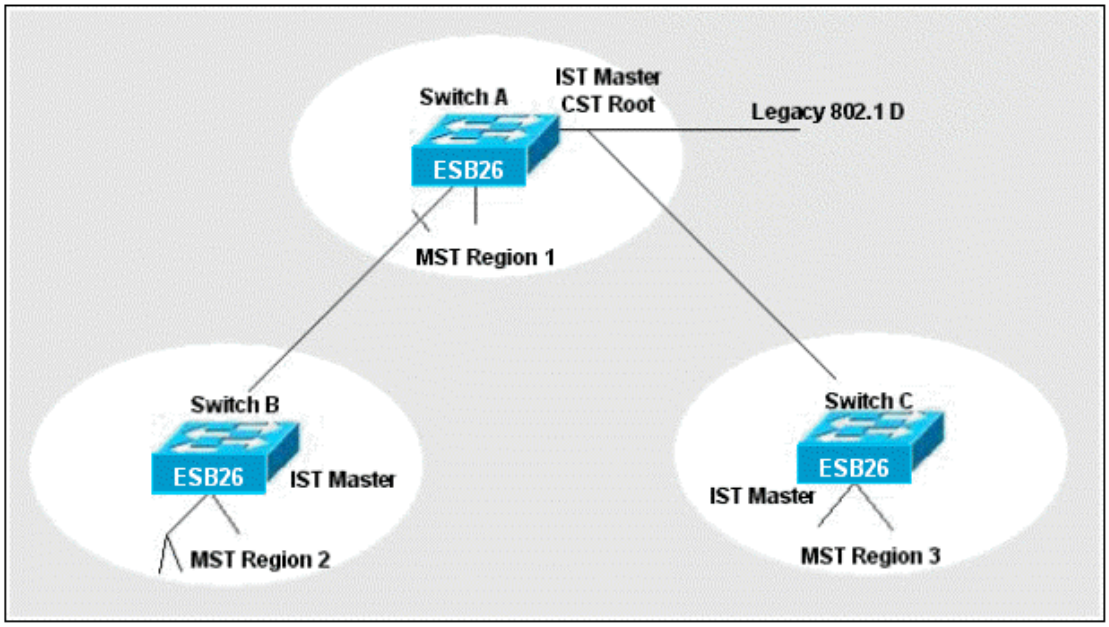


Figure 14-2 MST Regions, IST Masters, and the CST Root

Figure 14-2 does not show additional MST instan

ces for each region. Note that the topology of MST instances can be different from that of the IST for the same region.

Only the CST instance sends and receives BPDUs, and MST instances add their spanning-tree information into the BPDUs to interact with neighboring switches and calculate the final spanning-tree topology. Because of this, the spanning-tree parameters related to BPDU transmission (for example, **hello-time**, **forward-delay**, **max-age**, and **max-hops**) are configured only on the CST instance but affect all MST instances. Parameters related to the spanning-tree topology (for example, **switch priority**, **port cost**, **port priority**) can be configured on both the CST instance and the MST instance.

The IST and MST instances do not use the message-age and maximum-age information in the configuration BPDU to compute the spanning-tree topology. Instead, they use the path cost to the root and a hop-count mechanism similar to the IP time-to-live (TTL) mechanism.

By using the **mstp max-hops** command, in Protocol Configuration mode, you can configure the maximum hops inside the region and apply it to the IST and all MST instances in that region. The hop count achieves the same result as the message-age information (determines when to trigger a reconfiguration). The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs it generates. When the count reaches zero, the switch discards the BPDU and ages the information held for the port.

The message-age and maximum-age information in the RSTP portion of the BPDU remain the same throughout the region, and the region's designated ports at the boundary propagate the same values.

MST-to-SST Interoperability

A virtual bridged LAN may contain interconnected regions of SST and MST bridges.

To enable running STP in the SST region, an MST region appears as a single SST or pseudobridge, which operates as follows:

- Although the values for root identifiers and root path costs match for all BPDUs in all pseudobridges, a pseudobridge differs from a single SST bridge as follows:
    - The pseudobridge BPDUs have different bridge identifiers. This difference does not affect STP operation in the neighboring SST regions because the root identifier and root cost are the same.
    - BPDUs sent from the pseudobridge ports may have significantly different message ages. Because the message age increases by one second for each hop, the difference in the message age is measured in seconds.
- Data traffic from one port of a pseudobridge (a port at the edge of a region) to another port follows a path entirely contained within the pseudobridge or MST region. Data traffic belonging to different VLANs might follow different paths within the MST regions established by MST.
- The system prevents looping by doing either of the following:
    - Blocking the appropriate pseudobridge ports by allowing one forwarding port on the boundary and blocking all other ports
    - Setting the CST partitions to block the ports of the SST regions.

MST Instances

BiNOS supports up to 16 instances. Each spanning tree instance is identified by an instance ID that ranges from 0 to 15. Instance 0 is mandatory and is always present. Instances 1 through 15 are optional.

MST Region Overview

Interconnected bridges that have the same MST configuration are referred to as an MST region. There is no limit on the number of MST regions in the network.

To form an MST region, bridges can be either of the following:

- An MST bridge that is the only member of the MST region.
- An MST bridge interconnected by a LAN. A LAN's designated bridge has the same MST configuration as an MST bridge. All the bridges on the LAN can process MST BPDUs.

If you connect two MST regions with different MST configurations, the MST regions do the following:

- Load balance across redundant paths in the network. If two MST regions are redundantly connected, all traffic flows on a single connection with the MST regions in a network.

- Provide an RSTP handshake to enable rapid connectivity between regions. However, the handshaking is not as fast as between two bridges. To prevent loops, all the bridges inside the region must agree upon the connections to other regions. This situation introduces a delay. We do not recommend partitioning the network into a large number of regions.

Boundary Ports

A boundary port is a port that connects to a LAN, the designated bridge of which is either an SST bridge or a bridge with a different MST configuration. A designated port knows that it is on the boundary if it detects an STP bridge or receives an agreement message from an RST or MST bridge with a different configuration.

At the boundary, the role of MST ports do not matter, their state is forced to be the same as the IST port state. If the boundary flag is set for the port, the MSTP Port Role selection mechanism assigns a master port role to the port and the same state as that of the IST port. The IST port at the boundary can take up any port role except a backup port role.

IST Master

The IST master of an MST region is the bridge with the lowest bridge identifier and the least path cost to the CST root. If an MST bridge is the root bridge for an MST instance, then it is the IST master of that MST region. If the CST root is outside the MST region, then one of the MST bridges at the boundary is selected as the IST master. Other bridges on the boundary that belong to the same region eventually block the boundary ports that lead to the root.

If two or more bridges at the boundary of a region have an identical path to the root, you can set a slightly lower bridge priority to make a specific bridge the IST master.

The root path cost and message age inside a region stay constant, but the IST path cost is incremented and the IST remaining hops are decremented at each hop.

Regional Root

The root bridge of each MSTI in a region is referred to as the MSTI's regional root. In the case of the IST (MSTI0), it is referred to as the CIST Regional root. Therefore, the terms "IST Master" and "CIST Regional root" are interchangeable.

Edge Ports

A port that is connected to a nonbridging device (for example, a host or a switch) is an edge port. A port that connects to a hub is also an edge port if the hub or any LAN that is connected to it does not have a bridge. An edge port can start forwarding as soon as the link is up.

MSTP requires that you configure each port connected to a host. To establish rapid connectivity after a failure, you need to block the non-edge designated ports of an intermediate bridge. If the port connects to another bridge that can send back an agreement, then the port starts forwarding immediately. Otherwise, the port needs twice the forward delay time to start forwarding again. You must explicitly configure the ports that are connected to the hosts and switches as edge ports while using MSTP.

Link Type

Rapid connectivity is established only on point-to-point links. If you connect a port to another port through a point-to-point link and the local port becomes a designated port, the RSTP negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology. By default, the link type is automatically determined by the duplex state of the port. If you have a half-duplex link physically connected point-to-point to a single port on a remote switch running RSTP, you can override the default setting of the link type and enable rapid transitions to the forwarding state.

Message Age and Hop Count

IST and MST instances do not use the message age and maximum age timer settings in the BPDU. IST and MST use a separate hop count mechanism that is very similar to the IP time-to live (TTL) mechanism. You can configure each MST Bridge with a maximum hop count. The root bridge of the instance sends a BPDU (or M-record) with the remaining hop count that is equal to the maximum hop count. When a bridge receives a BPDU (or M-record), it decrements the received remaining hop count by one. The bridge discards the BPDU (M-record) and ages out the information held for the port if the count reaches zero after decrementing. The nonroot bridges propagate the decremented count as the remaining hop count in the BPDUs (M-records) they generate.

The message age and maximum age timer settings in the RST portion of the BPDU remain the same throughout the region, and the region's designated ports at the boundary propagate the same values.

Port Priority

The MSTP uses the port priority when selecting an interface to put into the forwarding state if a loop occurs. To interfaces that you want selected first, you can assign higher priority values, and to interfaces that you want selected last you can assign lower priority values. A higher priority value corresponds to a lower numerical value and a lower priority value corresponds to a higher numerical value. If all interfaces have the same priority value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Path Cost

The MSTP uses path cost when selecting an interface to put in the forwarding state if a loop occurs. The MSTP path cost default value is derived from the link speed of an interface. You can assign lower cost values that you want selected first and higher cost values to interfaces that you want selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Interoperability with 802.1D STP

A switch running both MSTP and RSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MST switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2). However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the

designated switch. Also, a switch might continue to assign a boundary role to a port when the switch to which it is connected has joined the region.

If all the legacy switches on the link are RSTP switches, they can process MSTP BPDUs as if they are RSTP BPDUs. Therefore, MSTP switches send either a version 0 configuration and TCN BPDUs or version 3 MSTP BPDUs on a boundary port. A boundary port connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

Benefits

- MSTP enables load balancing, over a large number of VLANs.
- MSTP reduces the number of spanning-tree instances required to support a large number of VLANs by using VLAN grouping.
- MSTP provide rapid convergence, which can reduce link convergence time to less than two seconds.
- MSTP continues operating without loops in any physical connection topology including shared spanning tree switches, 802.1Q mono spanning tree switches, and others.

Supported Standards, MIBs and RFCs

Standards

IEEE 802.1D-1998

IEEE 802.1W-2001

IEEE 802.1S-2002

MIBs

Private MIB, *batm_mst.mib*

RFCs

No RFCs are supported by this feature.

Prerequisites

The MSTP implementation operates over MSTIs which are, in turn, mapped into groups of VLANs. However, since the MSTP does not enforce VLAN membership state for ports, a situation of inconsistency between the MSTP port's state and the real state of the port may arise. For example, MSTP may set a port state on MSTI3 to be forwarding, when the instance is mapped to VLANs 3-5. If the port is not a member of VLAN 4, it will effectively be blocked on that VLAN, although the MSTP will show a forwarding state.

Make sure that this consistency is maintained, either by matching the VLAN memberships to the MSTP state or by changing MSTP parameters (such as path-cost and priority) so the traffic will be diverted to correct ports.

Default MSTP Configuration

Table 14-2 lists the MSTP default parameter values.

Table 14-2 MSTP Default Parameter Values

Parameter	Default Value
Multiple Spanning tree mode (MSTP)	Disabled
Spanning tree port priority	128
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds
Maximum hop count	40 hops
Revision number	1
Default MTS Instance	0
Bridge priority	32768
Path cost	See table 14-3

Edge Port	Disable
Link Type	Auto
Cisco MSTP compliance	Disable (IEE 802.1s-2002 compliance is enabled)
MSTP debug	Disable

Table 14-3 Default Path Cost Values (IEEE8021s)

Link Speed	Recommended Value	Recommended Range	Range
<=100 Kbps	200,000,000	20,000,000-200,000,000	1-200,000,000
1 Mbps	20,000,000	2,000,000-20,000,000	1-200,000,000
10 Mbps	2,000,000	200,000-2,000,000	1-200,000,000
100 Mbps	200,000	20,000-200,000	1-200,000,000
1 Gbps	20,000	2,000-200,000	1-200,000,000
10 Gbps	2,000	200-20,000	1-200,000,000
100 Gbps	200	20-2,000	1-200,000,000
1 Tbps	20	2-200	1-200,000,000
10 Tbps	2	1-20	1-200,000,000

Configuring and Displaying MSTP

Configuring Global MSTP Parameters

Table 14-4 lists the MSTP global configuration commands.

Table 14-4 MSTP Configuration Commands

Command	Description
mstp	Enables/disables the MSTP, or changes the mode from Protocol Configuration to Protocol MSTP Configuration mode.
name	Defines the configuration name
revision	Defines the configuration revision
abort	Exits the configuration without saving the MST configuration map.
apply	Saves the MST configuration map and exits the configuration.
mstp hello-time	Sets the hello time.
mstp forward-delay	Sets the time for forward delay.
mstp max-age	Sets the maximum aging time.
mstp max-hops	Defines the max hop count.
mstp hold-count	Sets the MSTP transmit holdcounter.

Enabling MSTP

The **mstp** command, in Protocol Configuration mode, enables the MSTP when the **enable** argument is specified, disables the MSTP when the **disable** argument is specified, and enters into Protocol MSTP Configuration mode if no argument is specified.

By default, MSTP is disabled.

Command Syntax

```
device-name(cfg protocol)#mstp [enable|disable]
```

Argument Description

enable	Enables the MSTP.
disable	Disables the MSTP.

Example

The following Example displays how to enter into Protocol MSTP Configuration mode:

```
device-name(cfg protocol)#mstp
device-name(cfg protocol mstp)#
```

Setting the Configuration Name

The **name** command, in Protocol MSTP Configuration mode, sets the MST region name. The **no** form of this command removes the configured MST region name.

Command Syntax

```
device-name(cfg protocol mstp)#name NAME
device-name(cfg protocol mstp)#no name
```

Argument Description

NAME	The configuration name. The name length up to 31 characters (case sensitive).

Example

```
device-name(cfg protocol mstp)#name region1
```

Setting the Configuration Revision

The **revision** command, in Protocol MSTP Configuration mode, sets the MST configuration revision number. The **no** form of this command returns to the default revision number.

By default, the revision number is 1.

Command Syntax

```
device-name(cfg protocol mstp)#revision <revision-number>
device-name(cfg protocol mstp)#no revision
```

Argument Description

revision-number	The MST configuration revision number in the range <0-65535>.

Example

```
device-name(cfg protocol mstp)#revision 1
```

Terminating the Configuration without Storing the MST Map

The **abort** command, in Protocol MSTP Configuration mode, exits Protocol MSTP Configuration mode without saving the MST configuration map.

When the **abort** command is used, the changes in the VLAN ID to MSTI mapping will not be saved. To save the changes in the VLAN ID to MSTI mapping, use the **apply** command in Protocol MSTP Configuration mode.

NOTE The apply command has the same effect as the exit command, or the shortcut key <Ctrl+D>.

Command Syntax

```
device-name(cfg protocol mstp)#abort
```

Storing the MST Map and Terminating the Configuration

The **apply** command, in Protocol MSTP Configuration mode, saves the MST configuration map and exits Protocol Configuration MSTP mode.

When using the **apply** command, the changes in the VLAN ID to MSTI mapping will be saved. If you do not want to save the changes in the VLAN ID to MSTI mapping, use the **abort** command in Protocol MSTP Configuration mode.

NOTE The apply command has the same effect as the exit command, or the shortcut key <Ctrl+D>.

Command Syntax

```
device-name(cfg protocol mstp)#apply
```

Setting the Hello Time

The **mstp hello-time** command, in Protocol Configuration mode, configures hello time for all MST instances. The **no** form of this command resets the hello time to its default setting.

The hello time is the interval between the generations of configuration messages by the root switch. These messages indicate that the switch is alive.

By default, the hello time value is 2 seconds.

Command Syntax

```
device-name(cfg protocol)#mstp hello-time <seconds>
device-name(cfg protocol)#no mstp hello-time
```

Argument Description

seconds	The MSTP hello time in seconds. The range is <1-10>.

Setting the Forward Delay Time

The **mstp forward-delay** command, in Protocol Configuration mode, configures the forward time for all MST instances. The **no** form of this command resets the value to its default.

The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.

By default, the forward delay time is 15 seconds.

Command Syntax

```
device-name(cfg protocol)#mstp forward-delay <seconds>
device-name(cfg protocol)#no mstp forward-delay
```

Argument Description

seconds	The RSTP forward delay time in seconds. The range is <4-30>.

Setting the Maximum Aging Time

The **mstp max-age** command, in Protocol Configuration mode, configures the maximum-aging time for all MST instances. The **no** form of this command resets the time value to its default setting.

The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

By default, the time value is 20 seconds.

Command Syntax

```
device-name(cfg protocol)#mstp max-age <seconds>
device-name(cfg protocol)#no mstp max-age
```

Argument Description

seconds	Sets the RSTP maximum age time. The range is <6-40>.

Setting the Switch Maximum Hop Count

The **mstp max-hops** command, in Protocol Configuration mode, specifies the number of hops in a region before the BPDU is discarded, and the information held for a port is aged. The **no** form of this command resets the value to its default setting.

By default, the max hop count is set to 40.

Command Syntax

```
device-name(cfg protocol)#mstp max-hops <hops-count>
device-name(cfg protocol)#no mstp max-hops
```

Argument Description

hops-count	The number of hops in a region. The range is <1- 40>.

Setting the MSTP Hold Counter

The **mstp hold-count** command, in Protocol Configuration mode, specifies the maximim number of packets that can be sent for a hello time period. The **no** form of this command resets the value to its default setting.

By default, the MSTP hold counter is set to 3.

Command Syntax

```
device-name(cfg protocol)#mstp hold-count <packets-count>
device-name(cfg protocol)#no mstp hold-count
```

Argument Description

packets-count	The maximum number of allowed for a hello time period. The range is 3- 20.

Configuring MSTI Parameters

Table 14-5 lists the MSTI configuration commands.

Table 14-5 MSTI Configuration Commands

Command	Description
instance vlan	Maps an MSTP instance to a VLAN.
mstp priority	Sets the MSTP priority.

Mapping an MST Instance to a VLAN

The **instance vlan** command, in Protocol MSTP Configuration mode, maps VLANs to an MST instance. The **no** form of this command unmaps all the VLANs that were mapped to an MST instance.

BiNOS supports up to 16 instances. Each spanning tree instance is identified by an instance ID that ranges from 0 to 15. Instance 0 is mandatory and is always present. Instances 1 through 15 are optional.

When you map VLANs to an MST instance, the specified VLANs are added to or removed from the existing list.

To specify a VLAN range, use a hyphen. For example, **instance 1 vlan 1-63** maps VLANs 1 through 63 to MST instance 1.

To specify a list of VLANs, use a comma. The list must be entered in increasing order of ID numbers. For example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

Command Syntax

```
device-name(cfg protocol mstp)#instance <instance-id> vlan VLAN-LIST
device-name(cfg protocol mstp)#no instance <instance-id>
```

NOTES

1. The VLAN blocking is implemented by removing the port internally from that VLAN. This can cause InErrors counter of such port to increase in cases of flooding or when port changes its role due to topology changes.
2. When port is member of tagged VLAN – the secure block port feature should be used.

Argument Description

instance-id	The MST instance ID. The range is 1 to 15.
VLAN-LIST	The list of VLANs to add to the instance mapping. The range of values is <1-4094>.

Setting the Bridge Priority

The **mstp priority** command, in Protocol Configuration mode, sets the bridge priority for an MST instance. The **no** form of this command resets the switch priority for the MST instance.

Command Syntax

```
device-name(cfg protocol)#mstp <instance-id> priority <priority>
device-name(cfg protocol)#no mstp <instance-id> priority
```

Argument Description

instance-id	The MST instance ID. The range is 0 to 15.
priority <priority>	Determines the likelihood that the switch will be chosen as the root switch. The range is 0 (highest likelihood) to 61440 (lowest likelihood) at increments of 4096. The default priority value is 32768. The valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Configuring the MSTP Interface Parameters

Table 14-6 lists the MSTP interface configuration commands.

Table 14-6 MSTP Interface Configuration Commands

Command	Description
mstp port priority	Sets the MSTP port priority.
mstp path-cost	Sets the path cost of the MSTP port.
mstp edge-port	Sets the edge port.
mstp link-type	Specifies the type of the link.
mstp default	Sets the default MSTP port.
mstp detect-protocols	Forces the port to work by the Rapid Spanning Tree Protocol (RSTP) and not by the Spanning Tree Protocol (STP).
mstp cisco-compliant	Enables the port to work with Cisco-compliant devices.

Setting the MSTP Port Priority

The **mstp port priority** command, in Interface Configuration mode, defines the MST port priority. The **no** form of this command returns the interface to its default settings.

By default, the spanning tree port priority is 128.

If a loop occurs, the MSTP uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces to be selected first and lower priority values (higher numerical values) to interfaces to be selected last. If all interfaces have the same priority value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Command Syntax

```
device-name(config-if UU/SS/PP)#mstp <instance-id> port-priority <priority>
device-name(config-if UU/SS/PP)#no mstp <instance-id> port-priority
```

Argument Description

instance-id	The MST instance ID. The range is <0-15>.

port-priority <priority>	The port priority value, range is 0 (highest priority) to 255 (lowest priority). The default is 128.

Example

```
device-name(config)#interface ag2
device-name(config-if AG02)#mstp 0 port-priority
  0   112   128   144   16   160   176   192   208   224   240   32   48   64   80   96
device-name(config-if AG02)#mstp 0 port-priority 208
device-name(config-if AG02)#
```

NOTE The port-priority command can be used on aggregate ports as well, as shown in the example above. In such cases, the reference ag is included in the instance ID preceeding the ID number

Setting the Path Cost

The **mstp path-cost** command, in Interface Configuration mode, configures the cost for an MST instance. The **no** form of this command returns the interface to its default settings.

If a loop occurs, the MSTP uses the path cost when selecting an interface to place in the forwarding state. A lower path cost represents higher-speed transmission

The default MSTP path cost value is derived from the link speed of an interface. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want to be selected first and higher cost values that you want to interfaces to be selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

The default value is derived from the link speed of the interface. Table 14-3 displays the default value calculated from the media speed of the interface.

Command Syntax

```
device-name(config-if UU/SS/PP)#mstp <instance-id> path-cost <1-200000000>
device-name(config-if UU/SS/PP)#no mstp <instance-id> path-cost
```

Argument Description

instance-id	The MST instance ID, the range is 0 to 15.
<1-200000000>	The cost value, in the range <1-200000000>.

Example

```
device-name(config)#interface ag2
device-name(config-if AG02)#mstp 0 path-cost 1
device-name(config-if AG02)#
```

NOTE The **mstp path-cost** command can be used on aggregate ports as well, as shown in the example above. In such cases, the reference ag is included in the instance ID preceeding the ID number

Setting the Edge Port

The **mstp edge-port** command, in Interface Configuration mode, changes the admin status. The **no** form of this command disables the admin status.

The *EdgePort* parameter is controlled by the MSTP state machine and the Command Line Interface (CLI):

- ***Admin EdgePort***
  The admin *EdgePort* parameter can be set by the CLI on a per-Port basis in order to indicate that a given Port is permitted to transit directly to the Forwarding Port State when a Port becomes *Designated*.

  This functionality is provided in order to permit Bridge Ports that are (administratively) known to be at the edge of the Bridged LAN to transition to Forwarding without delay.

  However, as the presence of a Bridge on a Port that has been marked as an edge Port could potentially cause a loop in the active topology, it is necessary to qualify the value of the administrative state variable according to the port's knowledge of whether or not any BPDUs have been received on the Port.

- ***EdgePort***

  The Bridge Detection state machine controls the value of the corresponding operational state variable, operational EdgePort, which may be used in order to determine whether a port that becomes Designated is permitted to transit directly to Forwarding. A value of enabled in the show commands indicates that this state transition is permitted to occur.

  If a BPDU is received on the Port, then the value of operational EdgePort is set to disabled. Following a port initialization, or following a link-up event, operational EdgePort is set to the value of admin EdgePort.

  Hence, if a Port that has been marked as an edge-port proves not to be one (due to the presence of another Bridge), then it will cease to behave like an edge-port until such a time as it is reinitialized (either by a link up/down event or by reissuing the CLI command).

NOTE

If a BPDU is received on a port defined as an edge port, it automatically reverts to edge-port disabled status. After link up/down or after the edge port command is used, the port returns to the Admin status.

Command Syntax

```
device-name(config-if UU/SS/PP)#mstp edge-port
device-name(config-if UU/SS/PP)#no mstp edge-port
```

Setting the Link Type

The **mstp link-type** command, in Interface Configuration mode, sets the administrative status of the MSTP port's link state. The **no** form of the command resets the port's administrative link type to its default value (auto).

There are two statuses of link state: operational and administrative.

1. Admin Link-Type:

Auto

From the point of view of determining the value of the link-type, an MSTP port is considered to be connected to a point-to-point LAN segment if any of the following conditions are true:

a) The port's link-type is set to Auto, and the MST algorithm has determined that the LAN segment is to be operated in full duplex mode.

b) The port has been configured by management means for full duplex operation. Otherwise, the MAC is considered to be connected to a LAN segment that is not point-to-point (shared media).

Point-to-point

The port is considered to be connected to a point-to-point LAN segment which forces the operational link-type to be point-to-point.

Shared

The port is considered to be connected to a shared media LAN segment which forces the operational link-type to be Shared.

2. Operational link-type

If Admin link-type is set to Auto, then the value of Operational link-type is determined in accordance with the specific procedures defined for the switch entity concerned, as defined in Admin link-type (auto).

If these procedures determine that the port is connected to a point-to-point LAN segment, then Operational link-type is set to point-to-point, otherwise it is set to *Shared*.

In the absence of a specific definition of how to determine whether the port is connected to a point-to-point LAN segment or not, the value of link-type shall be *Shared*.

Command Syntax

```
device-name(config-if UU/SS/PP)#mstp link-type {point-to-point | shared |
auto}
```

Argument Description

point-to-point	Sets the MSTP link type to point-to-point.
shared	Sets the MSTP link type to shared.
auto	Sets the MSTP link type dynamically according to the duplex status.

Setting the Default MSTP

The **mstp default** command, in Interface Configuration mode, sets the MSTP port configuration to its default values.

Command Syntax

```
device-name(config-if UU/SS/PP)#mstp default
```

Forcing a Port to Work by the RSTP Protocol

The **mstp detect-protocols** command, in Interface Configuration mode, forces the port to work by the Rapid Spanning Tree Protocol (RSTP) and not by the Spanning Tree Protocol

(STP). The command forces renegotiation of the LAN's protocol MSTP/STP with the neighboring bridges.

Command Syntax

```
device-name(config-if UU/SS/PP)#mstp detect-protocols
```

Cisco Compliance

The Nokia implementation for Cisco compliance requires several changes in the BPDUs format and the way the devices operate in Cisco Compliant mode.

An agreement flag within BPDUs is not sent from the designated port, when the device is in Cisco compliant mode, even if the port is synced.

A port is considered synced, in Cisco compliant mode, if it has received a proposal on a point-to-point link (Cisco does not send agreement flag within its BPDUs to the designated port).

When the device is not in Cisco compliant mode, a root port is synced only if it recieves an agreement together with the proposal flag from the designated port. If the port is not synced, it does not perform fast transition.

Example Comparison Between Nokia ESB26 and Cisco BPDU Formats:

The following is an example of parsing two BPDUs. Table 14-7 displays a Nokia ESB26 generated BPDU that matches IEEE 802.1s. The BPDU includes two M-records. Table 14-8 displays an example of a Cisco BPDU.

NOTE

In Cisco compliance mode, Nokia ESB26 generates and parses BPDUs with the format of Cisco BPDUs as it is displayed in Table 14-8.

Before parsing the BPDUs, first are displayed the dumps - BiNOS dump and Cisco dump. The differences from the 802.1s specification in Table 14-8 are displayed bolded.

BiNOS Dump

```
01 80 c2 00 00 00 00 a0 12 11 29 92 00 89 42 42
03 00 00 03 02 4e 80 00 00 a0 12 11 29 92 00 00
00 00 80 00 00 a0 12 11 29 92 80 0b 00 00 14 00
02 00 0f 00 00 00 60 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 01 60 b0 d3 6e cc e1
45 40 14 da 65 22 bd 08 f3 cd 00 00 00 00 80 00
00 a0 12 11 29 92 28 4e 80 01 00 a0 12 11 29 92
00 00 00 00 80 80 28 4e 80 02 00 a0 12 11 29 92
00 00 00 00 80 80 28
```

Cisco Dump

```
01 80 c2 00 00 00 00 08 a3 37 f1 c1 00 84 42 42
03 00 00 03 02 68 60 00 00 07 eb d5 a2 00 00 00
00 00 60 00 00 07 eb d5 a2 00 80 01 00 00 14 00
02 00 0f 00 00 00 00 5a 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 64 b1 f4 bb 1f 3c
6d 4d a3 00 94 c1 11 b7 c0 92 60 00 00 07 eb d5
```

```
a2 00 00 00 00 00 14 00 01 69 60 01 00 07 eb d5 a2 00 80 01
14 00
```

Table 14-7 BiNOS BPDU Parsed Exactly According to IEEE 8021s

BPDU Field	Content
ETH Dest.	01 80 c2 00 00 00
ETH Src	00 a0 12 11 29 92
ETH Len	00 89
LLC	42 42 03
Protocol Identifier	00 00
Protocol version Identifier	03
BPDU type	02
CIST Flags	4e
CIST Root Identifier	80 00 00 a0 12 11 29 92
CIST Ext. Path Cost	00 00 00 00
CIST Regional Root Identifier	80 00 00 a0 12 11 29 92
CIST Port Identifier	80 0b
Message age	00 00
Max age	14 00
Hello Time	02 00
Forward Delay	0f 00
Version 1 length (should be 0)	00
Version 3 length (Mrecords total length)	00 60
MSTI configuration Identifier (Key, Revision, Name) 51 Bytes	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 60 b0 d3 6e cc e1 45 40 14 da 65 22 bd 08 f3 cd
CIST Internal Root Path Cost	00 00 00 00
CIST Bridge Identifier	80 00 00 a0 12 11 29 92
CIST Remaining hops	28
MSTI1	
Flags	4e

MSTI Regional Root Identifier	80 01 00 a0 12 11 29 92
MSTI Internal root path cost	00 00 00 00
MSTI Bridge Priority	80
MSTI Port Priority	80
MSTI Remaining hops	28
MSTI2	
Flags	4e
MSTI Regional Root Identifier	80 02 00 a0 12 11 29 92
MSTI Internal root path cost	00 00 00 00
MSTI Bridge Priority	80
MSTI Port Priority	80
MSTI Remaining hops	28

Table 14-8 Cisco BPDU parsed by a BiNOS device

Field name	Value	Note
ETH Dest.	01 80 c2 00 00 00	Matches the IEEE-802.1s
ETH Src	00 08 a3 37 f1 c1	
ETH Len	00 84	
LLC	42 42 03	
Protocol Identifier	00 00	
Protocol version Identifier	03	
BPDU type	02	
CIST Flags	68	
CIST Root Identifier	60 00 00 07 eb d5 a2 00	
CIST Ext. Path Cost	00 00 00 00	
CIST Bridge Identifier	60 00 00 07 eb d5 a2 00	
CIST Port Identifier	80 01	
Message age	00 00	
Max age	14 00	
Hello Time	02 00	
Forward Delay	0f 00	
Version 1 length (should be 0)	00	
Extra byte	00	Refer to the Note below.
Version 3 length (Mrecords total length)	00 5a	

MSTI configuration Identifier (Key, Revision, Name) 50 Bytes.	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 64 b1 f4 bb 1f 3c 6d 4d a3 00 94 c1 11 b7 c0 92	The first byte of the configuration is called selector, and is omitted (or over-ridden by the version 3 length field)
CIST Regional Root Identifier	60 00 00 07 eb d5 a2 00	The fields order is flipped.
CIST Internal Root Path Cost	00 00 00 00	
CIST Remaining hops – 2 bytes instead of 1.	14 00	Extra byte - Cisco BPDU with no MSTIs ends here and contains the extra byte.
MSTI1		The whole M-Record structure is different. In the 802.1s there is no MSTID field. The priority of the sending bridge and the port priority are sent without bridge ID and port ID of the sending bridge.
MSTID	01	
Flags	69	
MSTI Regional Root Identifier	60 01 00 07 eb d5 a2 00	
MSTI Internal root path cost	00 00 00 00	
MSTI Transmitting Bridge Idnetifier	60 01 00 07 eb d5 a2 00	
MSTI Port Identifier	80 01	
MSTI Remaining hops	14 00	

NOTE

If the Cisco BPDUs are parsed as specified in IEEE 802.1s standard, some offsets and shifts may cause wrong values for the M-records and for the matching fields that are located after the version 3 length - CIST Internal root path cost, CIST Bridge identifier, CIST remaining hops.

Displaying MSTP Configuration

Table 14-9 lists the MSTP Display commands.

Table 14-9 MSTP Display Commands

Command	Description
show pending	Displays the temporary configuration.
show	Displays the MSTP configuration.
show mstp configuration	Displays the MSTP configuration in the current region.
show mstp	Displays the whole MSTP configuration.
show mstp instance	Displays the configured instances.

Displaying the Temporary Configuration

The **show pending** command, in Protocol MSTP Configuration mode, displays the temporary Multiple Spanning Tree Protocol (MSTP) configuration. The configuration displayed includes the region name, the MTSP revision number and the VLAN ID to MSTI mapping.

Command Syntax

```
device-name(cfg protocol mstp)#show pending
```

Example

```
device-name(cfg protocol mstp)#show pending

Pending MST configuration
Name        region 1
Revision    1
Instance    Vlans mapped
--------- ----------------------------------------------------
 0                        1-4094
-------------------------------------------------------------
```

Displaying the Configuration

The **show** command, in Protocol MSTP Configuration mode, displays the current Multiple Spanning Tree Protocol (MSTP) configuration. The configuration displayed includes the region name, the MTSP revision number and the VLAN ID to MSTI mapping.

Command Syntax

```
device-name(cfg protocol mstp)#show
```

Example

```
device-name(cfg protocol mstp)#show
Pending MST configuration
Name   []
Revision 1
Instance   Vlans mapped
--------- ------------------
 0         1-10,12-13
 1         14-4094
 6         11
---------------------------
```

Displaying a Particular MSTP Configuration

The **show mstp configuration** command in Privileged (Enable) mode, displays the MSTP configuration in current region.

Command Syntax

```
device-name#show mstp configuration
```

Example

```
device-name#show mstp configuration

Name   [man]
Revision 56
Instance   Vlans mapped
--------- --------------
 0         1-10,12-13
 1         14-4094
 6         11
------------------------
```

Displaying the MSTP Configuration

The **show mstp** command, in Protocol MSTP Configuration mode and Privileged (Enable) mode, displays the MSTP configuration and the MSTP ports state. Table 14-10 describes the parameters displayed by the **show mstp** command.

Command Syntax

```
device-name(cfg protocol mstp)#show mstp
device-name#show mstp
```

Example

```
device-name(cfg protocol mstp)#show mstp

Multiple spanning trees    = enabled
ProtocolSpecification     = ieee8021s
Priority                  = 0
TimeSinceTopologyChange   = 0 (Sec)
TopChanges                = 0
CIST Root                 = 00001.00:A0:12:0F:2F:27
CIST Port                 = 01/01/02
CIST Cost                 = 200000
MaxAge                    = 20 (Sec)
HelloTime                 = 2  (Sec)
ForwardDelay              = 15 (Sec)
BridgeMaxAge              = 0  (Sec)
BridgeHelloTime           = 2  (Sec)
BridgeForwardDelay        = 15 (Sec)
ProtoMigratioDelay        = 3  (Sec)
MaxHopCount               = 40
TxHoldCount               = 3

MST00
VLAN mapped               = 1-2,4-4094
Regional Root             = This bridge is the root
RemainingHopCount         = 0
TopChanges                = 0
=================================================================
Port    |Pri|Prt role|State|PCost |DCost  |Designated bridge |DPrt
--------+---+--------+-----+------+-------+------------------+-------
01/01/02 128 Root     block  200000      0 00000.00A0120F2F27 128.006

MST01
VLAN mapped               = 3
Regional Root             = This bridge is the root
RemainingHopCount         = 40
TopChanges                = 0
```

```
Port     |Pri|Prt role|State|PCost  |DCost   |Designated bridge  |DPrt
--------+---+--------+-----+------+-------+-------------------+-------
01/01/02 128 Boundary  block 200000      0 32768.00A0120B0AFA 128.002
```

Table 14-10 MSTP Show Command Parameters

Parameter	Description
Multiple spanning trees	Indicates whether MSTP is enabled or disabled on the switch.
ProtocolSpecification	Displays the supported IEEE standard..
Priority	The bridge priority which is part of the bridge identifier.
TimeSinceTopologyChange	The count in seconds since tcWhile timer (Topology-Change State Machine timer, specified in IEEE 802.1s, 13.21) for any Port was non-zero.
TopChanges	The number of topology changes detected for all the MSTIs.
CIST Root	The CIST Regional Root Identifier. The Bridge Identifier of the current CIST Regional Root.
CIST Port	The port in the switch from which the traffic flows to the CIST root.
CIST Cost	The CIST Path Cost. The CIST path cost from the transmitting Bridge to the CIST Regional Root.
MaxAge	The maximum age in seconds of received protocol information before it is discarded.
HelloTime	The time interval in seconds between the transmissions of Configuration BPDUs by a Bridge that is attempting to become the Root or is the Root.
ForwardDelay	The forward time for all MST instances. The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.
BridgeMaxAge	The value of the Max Age parameter in seconds when the Bridge is the Root or is attempting to become the Root.
BridgeHelloTime	The value of the Hello Time parameter in seconds when the Bridge is the Root or is attempting to become the Root. This parameter is the time interval between transmissions of Topology Change Notification BPDUs towards the Root, when the Bridge is attempting to notify the Designated Bridge on the LAN to which its Root Port is attached of a topology change.
BridgeForwardDelay	The value of the Forward Delay parameter in seconds when the Bridge is the Root or is attempting to become the Root.
ProtoMigratioDelay	This value is used by the Protocol Migration Machine to limit transition between the port's states.

MaxHopCount	The number of hops in a region before the BPDU is discarded, and the information held for a port is aged.
TxHoldCount	The value used to limit the rate of at which packets are sent. This value is connected to the Port Transmit State Machine.
MST00	Indicates for the MST instance 0.
VLAN mapped	The VLAN mapping of the MSTI.
Regional Root	The MSTI regional root.
RemainingHopCount	The value is used to determine the scope of an MSTP region.
TopChanges	Counts the number of the topology changes occurred for the specified MSTI.

Displaying the MSTP Instances Configuration

The **show mstp instance** command, in Privileged (Enable) mode, displays the configured MST instances for a specified interface or all the switch's interfaces. Table 14-11 describes the parameters displayed by the **show mstp instance** command.

Command Syntax

```
device-name#show mstp instance {<instance-id> | all} [interface UU/SS/PP]
```

Argument Description

instance-id	The MST instance ID, the range is 0 to 15.
all	All instances
interface UU/SS/PP	(Optional) Settings of MSTP port specified by Unit/Slot/Port number.

Example

```
device-name#show mstp instance 0 interface 1/1/1

MST instance 0
Port Enable          = enabled
Port Priority        = 128
Port State           = forwarding
Forward Transitions = 34
Port Role            = Root
Port Path Cost       = 200000
CIST Root            = 24576.0009B7990300
ExternalPortPathCost= 200000
Designated Root      = This bridge is the regional root
Port Path Cost       = 200000
Designated Bridge    = 24576.0009B7990300
Designated Port Id   = 96.1
AdminEdgePort        = disabled
OperEdgePort         = disabled
AdminLink-Type       = PointToPoint
Link-Type            = PointToPoint
Running Version      = RSTP
```

Table 14-11 MSTP Show Instance Command Parameters

Parameter	Description
Port Enable	Indicates whether the port is enabled or disabled.
Port Priority	The port priority for this MST Instance.
Port State	The state of the port for this MST Instance.
Forward Transitions	The number of times the port has transitioned into forward state.
Port Role	The role of the port for this MST Instance.
Port Path Cost	The port path cost for this MST Instance.
CIST Root	The CIST Regional Root Identifier. The Bridge Identifier of the current CIST Regional Root..
ExternalPortPathCost	The external port path cost of this port.
Designated Root	The ID of the designated bridge.
Designated Path Cost	The designated bridge port path cost.
Designated Bridge	The ID of the designated bridge for this network.
Designated Port Id	The ID of the designated bridge port.
AdminEdgePort	The administrative settings for the edge port.
OperEdgePort	The current Edge port working mode.
AdminLink-Type	The administrative settings for the link type.
Link-Type	The current link type working mode.
Running Version	The running version is RSTP when the neighbor on this port is an RSTP or MSTP device. The running version is STP when the neighbor on this port is an STP device. The running version is Cisco Compatible when the user set Cisco compatible mode on this port.

MSTP Debugging

Table 14-12 lists the MSTP debugging commands. The debug commands are intended for support personnel use to monitor MSTP process in detail.

All MSTP information is displayed at debugging log level, so to be able to view the MSTP log messages you must have applied the **log trap debuging** command beforehand.

An example of the debug output is:

```
tMstPIM: 1970/01/01 03:43:59 : Root port is now 1/1/11
```

For more information about the debug commands see "*Debug Commands for Troubleshooting Network Problems*".

Table 14-12 MSTP Debug Commands

Command	Description
debug mstp flush	Displays the flushing (clearing) of the MAC address table when topology changes have occurred.
debug mstp roles	Displays logs of the port roles.
debug mstp handshake	Displays port handshaking logs.
debug mstp pim	Displays logs of the port information state machine.
debug mstp prt	Displays logs of the port role transition state machine.
debug mstp tcmdebug mstp bpdu	Displays logs of the topology change state machine.Displays logs for thereceived and transmitted BPDUs.
no debug mstp	Disables all debug actions in the MSTP.
show debug mstp	Displays the status of the current debug actions in the MSTP.

Debugging the MSTP Flushing of MAC Address Table

The **debug mstp flush** command, in Privileged (Enable) mode, activates the MAC address table flush debugging in the Multiple Spanning Tree Protocol (MSTP). Use the **no** form of this command to disable the display of MAC address table flush debugging.

The **debug mstp flush** command will not be saved after reload.

By default, MSTP flush debugging is disabled.

Command Syntax

```
device-name#debug mstp flush
device-name#no debug mstp flush
```

Example

```
device-name#debug mstp flush
tMstPRT: 1970/01/01 01:18:33 : MSTP Flushing MSTID 1 port AG03
```

Debugging the MSTP Port Roles

The **debug mstp roles** command, in Privileged (Enable) mode, displays logs of the port roles in the Multiple Spanning Tree Protocol (MSTP). Use the **no** form of this command to disable the port roles debugging.

The **debug mstp roles** command will not be saved after reload.

By default, MSTP port roles debugging is disabled.

Command Syntax

```
device-name#debug mstp roles {all | <instance-id>}
device-name#no debug mstp roles {all | <instance-id>}
```

Argument Description

all	Displays logs for all instances.
instance-id	The MST instance ID, the range is 0 to 15.

Example

```
device-name#debug mstp roles all
MST MSTI  1 Select-Port-Roles
tMstPIM: 1970/01/01 01:29:50 : ============================
tMstPIM: 1970/01/01 01:29:50 : This bridge is the root
tMstPIM: 1970/01/01 01:29:50 : Port 1/1/2 Is DesignatedPort
tMstPIM: 1970/01/01 01:29:50 : Port 1/1/3 Is DesignatedPort
tMstPIM: 1970/01/01 01:29:50 : Port 1/1/4 Is DesignatedPort
```

Debugging the MSTP Handshake

The **debug mstp handshake** command, in Privileged (Enable) mode, displays logs of the devices' handshaking in the Multiple Spanning Tree Protocol (MSTP). Use the **no** form of this command to disable the handshaking debugging.

The **debug mstp handshake** command will not be saved after reload.

By default, MSTP port handshake debugging is disabled.

Command Syntax

```
device-name#debug mstp handshake {all | <instance-id>}
device-name#no debug mstp handshake {all | <instance-id>}
```

Argument Description

all	Displays logs for all instances.
instance-id	The MST instance ID, the range is 0 to 15.

Example

```
device-name#debug mstp handshake all
tMstPRT: 1970/01/01 01:22:25 : Port AG03 msti  1 Synced
tMstPRT: 1970/01/01 01:22:25 : Port AG03 msti  2 Synced
```

Debugging the MSTP PIM

The **debug mstp pim** command, in Privileged (Enable) mode, displays logs of the Port Information state Machine (PIM) in the Multiple Spanning Tree Protocol (MSTP) for a specified port range. Use the **no** form of this command to disable the MSTP PIM debugging.

The **debug mstp pim** command will not be saved after reload.

By default, MSTP PIM debugging is disabled.

Command Syntax

```
device-name#debug mstp pim {all|flags|events|stats} from <Pa> to <Pz>
device-name#no debug mstp pim {all|flags|events|stats}
```

Argument Description

all	Displays logs of all three PIM options (flags, events, stats) for the specified port range.
flags	Displays only the PIM flags logs for the specified port range.
events	Displays only the PIM events logs for the specified port range.
stats	Displays only the PIM stats logs for the specified port range.
<P_a>	Number of the first port specifying the port range. The number must be in logical port number format.
<P_z>	Number of the last port specifying the port range. The number must be in logical port number format.

Example

```
device-name#debug mstp pim all from 19 to 20
tMstPIM: 1970/01/01 01:25:35 : PIM CURRENT -> RECEIVE port 20 mst 0
tMstPIM: 1970/01/01 01:25:35 : PIM RECEIVE -> REPEATED_DESIG port 20 mst 0
tMstPIM: 1970/01/01 01:25:35 : PIM REPEATED_DESIG->CURRENT port 20 mst 0
```

Debugging the MSTP BPDU

The **debug mstp bpdu** command, in Privileged (Enable) mode, displays information about the received and transmitted BPDUs packet in the Multiple Spanning Tree Protocol (MSTP). The **no** form of this command disables the display of the MSTP BPDU information.

The MSTP debug commands will not be saved after reload.

By default, the MSTP BPDU debugging is disabled.

Command Syntax

```
device-name#debug mstp bpdu {rx|tx|sanity-check validation} {all|UU/SS/PP}
device-name#no debug mstp bpdu {rx|tx|sanity-check|instance-id|validation} {all|UU/SS/PP}
```

Argument Description

rx	Indicates receive BPDUs.
tx	Indicates transmit BPDUs.
instance-id	The MST instance ID; the range is 0 to 15.
sanity-check	Debugs messages about the sanity checks of the packets.
validation	Debugs the validation of timer values contained in the BPDU.
all	Debugs the BPDUs for all interfaces.
UU/SS/PP	Debugs the BPDUs for the specified interface.

Example

```
device-name#debug mstp bpdu rx
MstPRX: 1970/01/01 02:11:46 : Rcvd Mstp bpdu on port 1/2/2
tMstPRX: 1970/01/01 02:11:46 : ------------------------------
tMstPRX: 1970/01/01 02:11:47 : BPDU Protocol = 0
tMstPRX: 1970/01/01 02:11:47 : BPDU Version = 3
tMstPRX: 1970/01/01 02:11:47 : BPDU Type = 2
tMstPRX: 1970/01/01 02:11:47 :
tMstPRX: 1970/01/01 02:11:47 : BPDU Flags = 0x6c
Multiple Spanning Tree Protocol (MSTP)
tMstPRX: 1970/01/01 02:11:47 : BPDU TcAck = 0
tMstPRX: 1970/01/01 02:11:47 : BPDU Agree = 1
tMstPRX: 1970/01/01 02:11:47 : BPDU Frwrd = 1
tMstPRX: 1970/01/01 02:11:48 : BPDU Learn = 0
tMstPRX: 1970/01/01 02:11:48 : BPDU Role = Designated(3)
tMstPRX: 1970/01/01 02:11:48 : BPDU Prop = 0
tMstPRX: 1970/01/01 02:11:48 : BPDU Tc = 0
tMstPRX: 1970/01/01 02:11:48 :
tMstPRX: 1970/01/01 02:11:48 : BPDU Root Id = 0xa071c41880330e12
```

Debugging the MSTP PRTM

The **debug mstp prt** command, in Privileged (Enable) mode, displays logs of the Port Role Transition state Machine in the Multiple Spanning Tree Protocol (MSTP) for a specified port range. Use the **no** form of this command to disable the MSTP PRTM debugging.

The **debug mstp prt** command will not be saved after reload.

By default, MSTP PRTM debugging is disabled.

Command Syntax

```
device-name#debug mstp prt {all|flags|events|stats} from <Pa> to <Pz>
device-name#no debug mstp prt {all|flags|events|stats}
```

Argument Description

all	Displays logs of all three PRTM options (flags, events, stats) for the specified port range.
flags	Displays only the PRTM flags logs for the specified port range.
events	Displays only the PRTM events logs for the specified port range.
stats	Displays only the PRTM stats logs for the specified port range.
<P_a>	Number of the first port specifying the port range. The number must be in logical port number format.
<P_z>	Number of the last port specifying the port range. The number must be in logical port number format.

Example

```
device-name# debug mstp prt all from 1 to 20
tMstPRT: 1970/01/01 01:28:27 : PRT eve E_mstAgreed port 20 mst 0
tMstPRT: 1970/01/01 01:28:27 : PRT ACTIVE_PORT -> ROOT port 20 mst 0
tMstPRT: 1970/01/01 01:28:27 : PRT ROOT -> ACTIVE_PORT port 20 mst 0t
```

Debugging the MSTP TCM

The **debug mstp tcm** command, in Privileged (Enable) mode, displays logs of the port Topology Change state Machine in the Multiple Spanning Tree Protocol (MSTP) for a specified port range. Use the **no** form of this command to disable the MSTP TCM debugging.

The **debug mstp tcm** command will not be saved after reload.

By default, MSTP TCM debugging is disabled.

Command Syntax

```
device-name#debug mstp tcm {all|flags|events|stats} from <Pa> to <Pz>
device-name#no debug mstp tcm {all|flags|events|stats}
```

Argument Description

all	Displays logs of all three TCM options (flags, events, stats) for the specified port range.
flags	Displays only the TCM flags logs for the specified port range.
events	Displays only the TCM events logs for the specified port range.
stats	Displays only the TCM stats logs for the specified port range.
<P_a>	Number of the first port specifying the port range. The number must be in logical port number format.
<P_z>	Number of the last port specifying the port range. The number must be in logical port number format.

Example

```
device-name# debug mstp tcm all from 1 to 20
tMstPRT: 1970/01/01 16:02:53 : TCM INACTIVE -> INACTIVE port 20 mst 2
tMstPRT: 1970/01/01 16:02:53 : TCM DETECTED -> ACTIVE port 18
```

Disabling MSTP Ports Debug Information

The **no debug mstp** command, in Privileged (Enable) mode, used without arguments, disables displaying of MSTP debug information all debug processes. The command is effective if any MSTP ports debugging has been enabled. (By default, MSTP ports debugging is disabled.)

Command Syntax

```
device-name#no debug mstp {roles | handshake } {all | instance-id}
```

Argument Description for Roles/Handshake

roles	Disables displaying logs of the MSTP port roles.
handshake	Disables displaying logs of the devices' MSTP handshaking.
all	Disables displaying logs for all instances.
instance-id	Disables displaying logs for the specified MST instance ID; the range is 0 to 15.

Example

```
device-name#debug mstp roles all
tSpanRecv: 1970/01/01 02:27:14 : link up on port 1/1/1
tMstPIM: 1970/01/01 02:27:14 :
                                        MST Cist Select-Port-Roles
                                        ==========================
tMstPIM: 1970/01/01 02:27:14 : This bridge is the root
tMstPIM: 1970/01/01 02:27:14 : Port 1/1/1 Is DesignatedPort
tMstPIM: 1970/01/01 02:27:14 : Port 1/1/2 Is DesignatedPort
tMstPIM: 1970/01/01 02:27:14 :
                                  End-Roles-Selection
```

Displaying the MSTP Debugging

The **show debug mstp** command, in Privileged (Enable) mode, displays the status of the debug actions in the Multiple Spanning Tree Protocol (MSTP) that are currently active in the switch.

Command Syntax

```
device-name#show debug mstp
```

Example

```
device-name#show debug mstp

MSTP debugging status:

|MSTI |Dbg Role|Dbg Handshake|Dbg Flush
|0    |ON      |ON           |OFF      |
Port debugging status:

|Port  |Dbg RX|Dbg TX|Dbg Validation|Dbg Sanity|
|1/1/1 |OFF   |ON    |OFF           |OFF       |
|1/1/2 |OFF   |ON    |OFF           |OFF       |
|1/1/3 |OFF   |ON    |OFF           |OFF       |
|1/1/4 |OFF   |ON    |OFF           |OFF       |
|1/1/5 |OFF   |ON    |OFF           |OFF       |
```

Configuration Examples

Pending Configuration

The following example shows how to configure MSTP and display the temporary (pending) configuration.

1. Enter into Protocol MSTP Configuration mode and map the VLANs ranging from 1 to 10 to MST instance 1:

```
device-name#configure terminal
device-name(config)#protocol
```

```
device-name(cfg protocol)#mstp
device-name(cfg protocol mstp)#instance 1 vlan 1-10
```

2. Assign to the MSTP region the **name** *region 1* and the **revision** number *1*:

```
device-name(cfg protocol mstp)#name region1
device-name(cfg protocol mstp)#revision 1
```

3. Display the temporary (pending) configuration:

```
device-name(cfg protocol mstp)#show pending

Pending MST configuration
Name   [region1]
Revision 1
Instance   Vlans mapped
--------- -------------------------------------------------
 0         11-4094
 1         1-10
```

MSTP Port Configuration

The following example shows how to configure MSTP on interface 1/1/1 and how to display the configuration.

1. Enter into interface 1/1/1 configuration mode:

```
device-name#configure terminal
device-name(config)#interface 1/1/1
```

2. Assign **port priority** *2* to instance *1*, and **path cost** *22* to instance *2*:

```
device-name(config-if 1/1/1)#mstp 1 port-priority 2
device-name(config-if 1/1/1)#mstp 2 path-cost 22
device-name(config-if 1/1/1)#end
```

3. Display the MSTP port configuration:

```
device-name#show mstp instance all interface 1/1/1

MST instance 0
Port Enable                = enabled
Port Priority              = 128
Port State                 = forwarding
Forward Transitions        = 3
Port Role                  = Designated
Port Path Cost             = 200000
CIST Root                  = 00000.00A0120F2F27
ExternalPortPathCost       = 200000
Designated Root            = This bridge is the regional root
Port Path Cost             = 200000
Designated Bridge          = 32768.00A01211227A
Designated Port Id         = 128.1
AdminEdgePort              = disabled
OperEdgePort               = disabled
AdminLink-Type             = PointToPoint
Link-Type                  = PointToPoint

MST instance 1
Port Enable                = enabled
Port Priority              = 0
Port State                 = forwarding
```

```
Forward Transitions          = 1
Port Role                    = Root
Port Path Cost               = 200000
CIST Root                    = 00000.000000000000
ExternalPortPathCost         = 200000
Designated Root              = 32768.00A012110708
Port Path Cost               = 200000
Designated Bridge            = 32768.00A01211227A
Designated Port Id           = 128.2
AdminEdgePort                = disabled
OperEdgePort                 = disabled
AdminLink-Type               = PointToPoint
Link-Type                    = PointToPoint
```

MSTP Global Parameters Configuration

The following example shows how to configure MSTP global parameters.

1. Enter into Protocol Configuration mode and set the **forward-delay** value to *5* seconds:

```
device-name#configure terminal
device-name(config)#protocol
device-name(cfg protocol)#mstp forward-delay 5
```

2. Configure the following parameters:

Hello-time to *4* seconds, **max-age time** to *34* seconds and **max-hop count** to *23*.

```
device-name(cfg protocol)#mstp hello-time 4
device-name(cfg protocol)#mstp max-age 34
device-name(cfg protocol)#mstp max-hops 23
device-name(cfg protocol)#end
```

3. Display the MSTP configuration:

```
device-name#show mstp

Multiple spanning trees  = enabled
ProtocolSpecification    = ieee8021s
Priority                 = 32768
TimeSinceTopologyChange  = 0 (Sec)
TopChanges               = 8
CIST Root                = 00001.00:A0:12:0F:2F:27
CIST Port                = 01/01/10
CIST Cost                = 200000
MaxAge                   = 20 (Sec)
HelloTime                = 2 (Sec)
ForwardDelay             = 5 (Sec)
BridgeMaxAge             = 0 (Sec)
BridgeHelloTime          = 4 (Sec)
BridgeForwardDelay       = 5 (Sec)
ProtoMigratioDelay       = 3 (Sec)
MaxHopCount              = 23
TxHoldCount              = 3
MST00
VLAN mapped              = 2-4094
Regional Root            = This bridge is the root
RemainingHopCount        = 23
TopChanges                  = 8
==========================================================================
Port    |Pri|Prt role|State|PCost |DCost |Designated bridge | Prt
--------+---+--------+-----+------+------+------------------+-------
01/01/01 128 Designat frwrd 200000 200000 32768.00A01211227A 128.001
01/01/10 128 Root     frwrd 200000 0      00000.00A0120F2F27 128.006
```

```
01/01/13 128 Designat frwrd 200000 200000 32768.00A01211227A 128.013
MST01
VLAN mapped                 = 1
Regional Root               = 32769.00:A0:12:11:07:08
RemainingHopCount           = 39
TopChanges                  = 4
==============================================================================
Port     |Pri|Prt role|State|PCost |DCost |Designated bridge |DPrt
---------+---+--------+-----+------+------+------------------+-------
01/01/01   0  Root     frwrd 200000   0    32768.00A01211227A 128.001
01/01/10 128 Boundary frwrd 200000   0    32768.00A01211227A 128.010
01/01/13 128 Designat frwrd 200000   0    32768.00A01211227A 128.013
```

Network Configuration

In the following example, four Nokia ESB26 switches are interconnected via VLANs V100 and V200 that are mapped to two MST instances on each switch. The example shows how redundancy is achieved with MSTP Figure 14-3 displays the connections schematically.

After configuring the network, the **show mstp** command is used on each switch to verify that the MST instances are configured correctly.

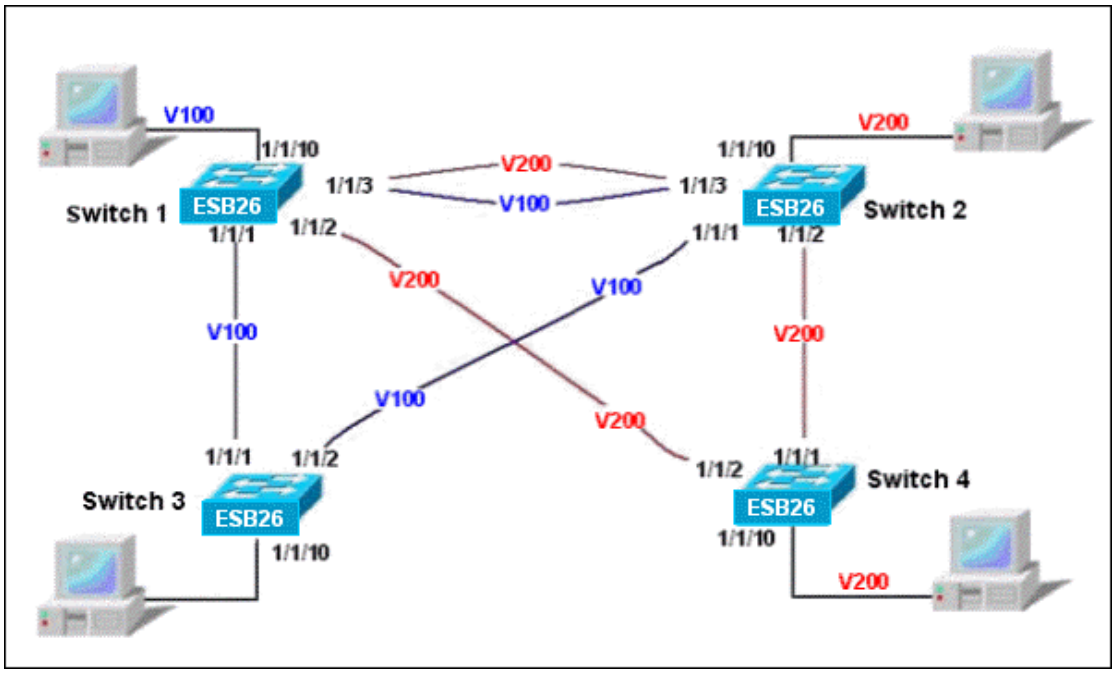


Figure 14-3 Schematic MSTI Configuration

Configuring Switch 1:

1. Create VLANs V100 and V200 and add the appropriate ports to each VLAN:

```
device-name#configure terminal
device-name(config)#vlan
device-name(config vlan)#config default
device-name(config-vlan default)# remove ports 1/1/1-1/1/3
device-name(config-vlan default)#exit
device-name(config vlan)#create v100 100
device-name(config vlan)#config v100
device-name(config-vlan v100)#add ports 1/1/1,1/1/3 tagged
device-name(config-vlan v100)#add ports 1/1/10 untagged
device-name(config-vlan default)#exit
```

```
device-name(config vlan)#create v200 200
device-name(config vlan)#config v200
device-name(config-vlan v200)#add ports 1/1/2,1/1/3 tagged
device-name(config-vlan v200)#exit
device-name(config vlan)#exit
```

2. Enter into Protocol Configuration mode and enable the MSTP:

```
device-name(config)#protocol
device-name(cfg protocol)#mstp enable
```

3. Set priority 0 to MSTI 1 in order to force ESB26 1 to be the root of MSTI1:

```
device-name(cfg protocol)#mstp 1 priority 0
```

4. Enter into Protocol MSTP Configuration mode:

```
device-name(cfg protocol)#mstp
```

5. Add VLANs to MTSIs 0, 1 and 2:

```
device-name(cfg protocol mstp)#instance 0 vlan 1-99,101-199,201-4094
device-name(cfg protocol mstp)#instance 1 vlan 100
device-name(cfg protocol mstp)#instance 2 vlan 200
```

Configuring Switch 2:

1. Create VLANs V100 and V200 and add the appropriate ports to each VLAN:

```
device-name#configure terminal
device-name(config)#vlan
device-name(config vlan)#config default
device-name(config-vlan default)# remove ports 1/1/1-1/1/3
device-name(config-vlan default)#exit
device-name(config vlan)#create v100 100
device-name(config vlan)#config v100
device-name(config-vlan v100)#add ports 1/1/1,1/1/3 tagged
device-name(config-vlan default)#exit
device-name(config vlan)#create v200 200
device-name(config vlan)#config v200
device-name(config-vlan v200)#add ports 1/1/2,1/1/3 tagged
device-name(config-vlan v200)#add ports 1/1/10 untagged
device-name(config-vlan v200)#exit
device-name(config vlan)#exit
```

2. Enter into Protocol Configuration mode and enable the MSTP:

```
device-name(config)#protocol
device-name(cfg protocol)#mstp enable
```

3. Set priority 0 to MSTI 2 in order to force ESB26 2 to be the root of MSTI2:

```
device-name(cfg protocol)#mstp 2 priority 0
```

4. Enter into Protocol MSTP Configuration mode:

```
device-name(cfg protocol)#mstp
```

5. Add VLANS to MTSIs 0, 1 and 2:

```
device-name(cfg protocol mstp)#instance 0 vlan 1-99,101-199,201-4094
device-name(cfg protocol mstp)#instance 1 vlan 100
device-name(cfg protocol mstp)#instance 2 vlan 200
```

Configuring Switch 3:

1. VLANs V100 and V200 are created on the switch and the appropriate ports are added to each VLAN:

```
device-name#configure terminal
device-name(config)#vlan
device-name(config vlan)#config default
device-name(config-vlan default)# remove ports 1/1/1,1/1/2,1/1/10
device-name(config-vlan default)#exit
device-name(config vlan)#create v100 100
device-name(config vlan)#config v100
device-name(config-vlan v100)#add ports 1/1/1,1/1/2 tagged
device-name(config-vlan v100)#add ports 1/1/10 untagged
device-name(config-vlan v100)#exit
device-name(config vlan)#exit
```

2. Enter into Protocol Configuration mode and enable the MSTP:

```
device-name(config)#protocol
device-name(cfg protocol)#mstp enable
```

3. Enter into Protocol MSTP Configuration mode:

```
device-name(cfg protocol)#mstp
```

4. Add VLANS to MTSIs 0, 1 and 2:

```
device-name(cfg protocol mstp)#instance 0 vlan 1-99,101-199,201-4094
device-name(cfg protocol mstp)#instance 1 vlan 100
device-name(cfg protocol mstp)#instance 2 vlan 200
```

Configuring Switch 4:

1. Create VLAN V200 and add the appropriate ports to the VLAN::

```
device-name#configure terminal
device-name(config)#vlan
device-name(config vlan)#config default
device-name(config-vlan default)# remove ports 1/1/1,1/1/2
device-name(config-vlan default)#exit
device-name(config vlan)#create v200 200
device-name(config vlan)#config v200
device-name(config-vlan v200)#add ports 1/1/1,1/1/2 tagged
device-name(config-vlan v200)#add ports 1/1/10 untagged
device-name(config-vlan v200)#exit
device-name(config vlan)#exit
```

2. Enter into Protocol Configuration mode and enable the MSTP

```
device-name(config)#protocol
device-name(cfg protocol)#mstp enable
```

3. Enter into Protocol MSTP Configuration mode:

```
device-name(cfg protocol)#mstp
```

4. Add VLANs to MTSIs 0, 1 and 2:

```
device-name(cfg protocol mstp)#instance 0 vlan 1-99,101-199,201-4094
device-name(cfg protocol mstp)#instance 1 vlan 100
device-name(cfg protocol mstp)#instance 2 vlan 200
```

After applying the configuration commands on all the switches as shown above and connecting the switches as shown in Figure 14-3, the following information will be displayed by the **show mstp** command on each of the switches:

Displaying the Configuration on Switch 1:

```
device-name#show mstp
Multiple spanning trees   = enabled
ProtocolSpecification     = ieee8021s
Priority                  = 0
TimeSinceTopologyChange   = 0 (Sec)
TopChanges                = 6
CIST Root                 = 32768.00:A0:00:01:09:0B
CIST Port                 = 01/01/03
CIST Cost                 = 0
MaxAge                    = 20 (Sec)
HelloTime                 = 2  (Sec)
ForwardDelay              = 15 (Sec)
BridgeMaxAge              = 20 (Sec)
BridgeHelloTime           = 2  (Sec)
BridgeForwardDelay        = 15 (Sec)
ProtoMigratioDelay        = 3  (Sec)
MaxHopCount               = 40
TxHoldCount               = 3

MST00
VLAN mapped               = 1-99,101-199,201-4094
Regional Root             = 32768.00:A0:00:01:09:0B
RemainingHopCount         = 39
TopChanges                = 6
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Designat frwrd    200000         0 32768.00A0120A0168 128.001
01/01/02 128 Designat frwrd    200000         0 32768.00A0120A0168 128.002
01/01/03 128 Root     frwrd    200000         0 32768.00A00001090B 128.003
01/01/10 128 Designat frwrd    200000         0 32768.00A0120A0168 128.010

MST01
VLAN mapped               = 100
Regional Root             = This bridge is the root
RemainingHopCount         = 40
TopChanges                = 5
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Designat frwrd    200000         0 00000.00A0120A0168 128.001
01/01/02 128 Designat frwrd    200000         0 00000.00A0120A0168 128.002
01/01/03 128 Designat frwrd    200000         0 00000.00A0120A0168 128.003
01/01/10 128 Designat frwrd    200000         0 00000.00A0120A0168 128.010

MST02
VLAN mapped               = 200
Regional Root             = 00002.00:A0:00:01:09:0B
RemainingHopCount         = 39
```

```
TopChanges                  = 7
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Designat frwrd    200000         0 32768.00A0120A0168 128.001
01/01/02 128 Designat frwrd    200000         0 32768.00A0120A0168 128.002
01/01/03 128 Root     frwrd    200000         0 00000.00A00001090B 128.003
01/01/10 128 Designat frwrd    200000         0 32768.00A0120A0168 128.010
```

Displaying the Configuration on Switch 2:

```
device-name#show mstp
Multiple spanning trees   = enabled
ProtocolSpecification     = ieee8021s
Priority                  = 0
TimeSinceTopologyChange   = 0 (Sec)
TopChanges                = 4
CIST Root                 = This bridge is the root
MaxAge                    = 20 (Sec)
HelloTime                 = 2  (Sec)
ForwardDelay              = 15 (Sec)
BridgeMaxAge              = 20 (Sec)
BridgeHelloTime           = 2  (Sec)
BridgeForwardDelay        = 15 (Sec)
ProtoMigratioDelay        = 3  (Sec)
MaxHopCount               = 40
TxHoldCount               = 3

MST00
VLAN mapped               = 1-99,101-199,201-4094
Regional Root             = This bridge is the root
RemainingHopCount         = 40
TopChanges                = 4
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Designat frwrd    200000         0 32768.00A00001090B 128.001
01/01/02 128 Designat frwrd    200000         0 32768.00A00001090B 128.002
01/01/03 128 Designat frwrd    200000         0 32768.00A00001090B 128.003
01/01/10 128 Designat frwrd    200000         0 32768.00A00001090B 128.010

MST01
VLAN mapped               = 100
Regional Root             = 00001.00:A0:12:0A:01:68
RemainingHopCount         = 39
TopChanges                = 4
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Designat frwrd    200000         0 32768.00A00001090B 128.001
01/01/02 128 Designat frwrd    200000         0 32768.00A00001090B 128.002
01/01/03 128 Root     frwrd    200000         0 00000.00A0120A0168 128.003
01/01/10 128 Designat frwrd    200000         0 32768.00A00001090B 128.010

MST02
VLAN mapped               = 200
Regional Root             = This bridge is the root
RemainingHopCount         = 40
TopChanges                = 4
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Designat frwrd    200000         0 00000.00A00001090B 128.001
01/01/02 128 Designat frwrd    200000         0 00000.00A00001090B 128.002
01/01/03 128 Designat frwrd    200000         0 00000.00A00001090B 128.003
01/01/10 128 Designat frwrd    200000         0 00000.00A00001090B 128.010
```

Displaying the Configuration on Switch 3:

```
device-name#show mstp
Multiple spanning trees   = enabled
ProtocolSpecification     = ieee8021s
Priority                  = 0
TimeSinceTopologyChange   = 0 (Sec)
TopChanges                = 3
CIST Root                 = 32768.00:A0:00:01:09:0B
CIST Port                 = 01/01/02
CIST Cost                 = 0
MaxAge                    = 20 (Sec)
HelloTime                 = 2  (Sec)
ForwardDelay              = 15 (Sec)
BridgeMaxAge              = 20 (Sec)
BridgeHelloTime           = 2  (Sec)
BridgeForwardDelay        = 15 (Sec)
ProtoMigratioDelay        = 3  (Sec)
MaxHopCount               = 40
TxHoldCount               = 3

MST00
VLAN mapped               = 1-99,101-199,201-4094
Regional Root             = 32768.00:A0:00:01:09:0B
RemainingHopCount         = 39
TopChanges                = 3
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Altern   block    200000         0 32768.00A0120A0168 128.001
01/01/02 128 Root     frwrd    200000         0 32768.00A00001090B 128.001
01/01/10 128 Designat frwrd    200000         0 32768.00A012BBBBBB 128.010

MST01
VLAN mapped               = 100
Regional Root             = 00001.00:A0:12:0A:01:68
RemainingHopCount         = 39
TopChanges                = 2
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Root     frwrd    200000         0 00000.00A0120A0168 128.001
01/01/02 128 Altern   block    200000         0 32768.00A00001090B 128.001
01/01/10 128 Designat frwrd    200000         0 32768.00A012BBBBBB 128.010

MST02
VLAN mapped               = 200
Regional Root             = 00002.00:A0:00:01:09:0B
RemainingHopCount         = 39
TopChanges                = 3
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Altern   block    200000         0 32768.00A0120A0168 128.001
01/01/02 128 Root     frwrd    200000         0 00000.00A00001090B 128.001
01/01/10 128 Designat frwrd    200000         0 32768.00A012BBBBBB 128.010
```

Displaying the Configuration on Switch 4:

```
device-name#show mstp
Multiple spanning trees    = enabled
ProtocolSpecification     = ieee8021s
Priority                  = 0
```

```
TimeSinceTopologyChange    = 0 (Sec)
TopChanges                 = 2
CIST Root                  = 32768.00:A0:00:01:09:0B
CIST Port                  = 01/01/01
CIST Cost                  = 0
MaxAge                     = 20 (Sec)
HelloTime                  = 2  (Sec)
ForwardDelay               = 15 (Sec)
BridgeMaxAge               = 20 (Sec)
BridgeHelloTime            = 2  (Sec)
BridgeForwardDelay         = 15 (Sec)
ProtoMigratioDelay         = 3  (Sec)
MaxHopCount                = 40
TxHoldCount                = 3

MST00
VLAN mapped                = 1-99,101-199,201-4094
Regional Root              = 32768.00:A0:00:01:09:0B
RemainingHopCount          = 39
TopChanges                 = 2
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Root     frwrd    200000         0 32768.00A00001090B 128.002
01/01/02 128 Altern   block    200000         0 32768.00A0120A0168 128.002
01/01/10 128 Designat frwrd    200000         0 32768.00A0120B0BC4 128.010

MST01
VLAN mapped                = 100
Regional Root              = 00001.00:A0:12:0A:01:68
RemainingHopCount          = 39
TopChanges                 = 5
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Altern   block    200000         0 32768.00A00001090B 128.002
01/01/02 128 Root     frwrd    200000         0 00000.00A0120A0168 128.002
01/01/10 128 Designat frwrd    200000         0 32768.00A0120B0BC4 128.010

MST02
VLAN mapped                = 200
Regional Root              = 00002.00:A0:00:01:09:0B
RemainingHopCount          = 39
TopChanges                 = 2
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/01 128 Root     frwrd    200000         0 00000.00A00001090B 128.002
01/01/02 128 Altern   block    200000         0 32768.00A0120A0168 128.002
01/01/10 128 Designat frwrd    200000         0 32768.00A0120B0BC4 128.010
```

If for example, the direct link between Switch 1 and Switch 3 fails (see Figure 14-4), MSTI01 is recalculated and port 1/1/2 in Switch 3 changes its role from alternate to root.

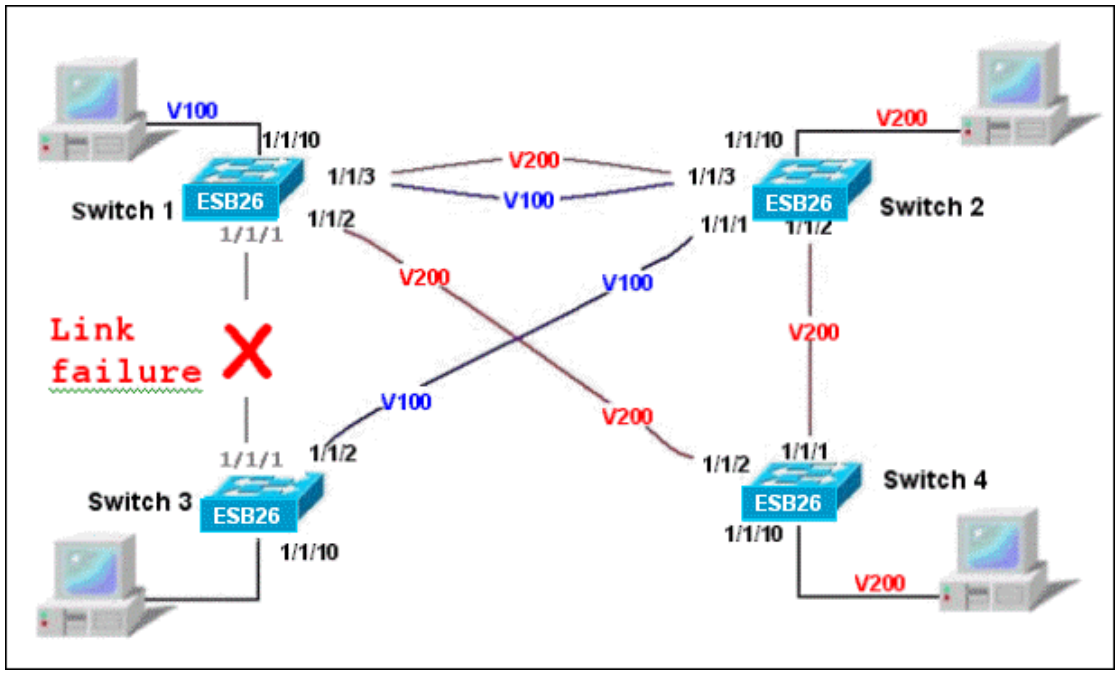


Figure 14-4 Link Failure Between Two Switches

In this case, the **show mstp** command will show the following.

On Switch 2 and Switch 4:

The output displayed by the **show mstp** command will not be affected by the change.

On Switch 1:

```
device-name#show mstp
Multiple spanning trees    = enabled
ProtocolSpecification      = ieee8021s
Priority                   = 0
TimeSinceTopologyChange    = 0 (Sec)
TopChanges                 = 6
CIST Root                  = 32768.00:A0:00:01:09:0B
CIST Port                  = 01/01/03
CIST Cost                  = 0
MaxAge                     = 20 (Sec)
HelloTime                  = 2  (Sec)
ForwardDelay               = 15 (Sec)
BridgeMaxAge               = 20 (Sec)
BridgeHelloTime            = 2  (Sec)
BridgeForwardDelay         = 15 (Sec)
ProtoMigratioDelay         = 3  (Sec)
MaxHopCount                = 40
TxHoldCount                = 3

MST00
VLAN mapped                = 1-99,101-199,201-4094
Regional Root              = 32768.00:A0:00:01:09:0B
RemainingHopCount          = 39
TopChanges                 = 6
================================================================================
Port     |Pri|Prt role|State|PCost     |DCost     |Designated bridge |DPrt
---------+---+--------+-----+----------+----------+------------------+-------
01/01/02 128 Designat frwrd    200000           0 32768.00A0120A0168 128.002
01/01/03 128 Root     frwrd    200000           0 32768.00A00001090B 128.003
01/01/10 128 Designat frwrd    200000           0 32768.00A0120A0168 128.010

MST01
```

```
VLAN mapped                 = 100
Regional Root               = This bridge is the root
RemainingHopCount           = 40
TopChanges                  = 5
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/02 128 Designat frwrd    200000         0 00000.00A0120A0168 128.002
01/01/03 128 Designat frwrd    200000         0 00000.00A0120A0168 128.003
01/01/10 128 Designat frwrd    200000         0 00000.00A0120A0168 128.010

MST02
VLAN mapped                 = 200
Regional Root               = 00002.00:A0:00:01:09:0B
RemainingHopCount           = 39
TopChanges                  = 7
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/02 128 Designat frwrd    200000         0 32768.00A0120A0168 128.002
01/01/03 128 Root     frwrd    200000         0 00000.00A00001090B 128.003
01/01/10 128 Designat frwrd    200000         0 32768.00A0120A0168 128.010
```

On Switch 3:

```
device-name#show mstp
Multiple spanning trees    = enabled
ProtocolSpecification      = ieee8021s
Priority                   = 0
TimeSinceTopologyChange    = 0 (Sec)
TopChanges                 = 3
CIST Root                  = 32768.00:A0:00:01:09:0B
CIST Port                  = 01/01/02
CIST Cost                  = 0
MaxAge                     = 20 (Sec)
HelloTime                  = 2  (Sec)
ForwardDelay               = 15 (Sec)
BridgeMaxAge               = 20 (Sec)
BridgeHelloTime            = 2  (Sec)
BridgeForwardDelay         = 15 (Sec)
ProtoMigratioDelay         = 3  (Sec)
MaxHopCount                = 40
TxHoldCount                = 3

MST00
VLAN mapped                = 1-99,101-199,201-4094
Regional Root              = 32768.00:A0:00:01:09:0B
RemainingHopCount          = 39
TopChanges                 = 3
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/02 128 Root     frwrd    200000         0 32768.00A00001090B 128.001
01/01/10 128 Designat frwrd    200000         0 32768.00A012BBBBBB 128.010

MST01
VLAN mapped                = 100
Regional Root              = 00001.00:A0:12:0A:01:68
RemainingHopCount          = 38
TopChanges                 = 3
================================================================================
Port    |Pri|Prt role|State|PCost    |DCost    |Designated bridge |DPrt
--------+---+--------+-----+---------+---------+------------------+-------
01/01/02 128 Root     frwrd    200000         0 32768.00A00001090B 128.001
01/01/10 128 Designat frwrd    200000         0 32768.00A012BBBBBB 128.010
```

```
MST02
VLAN mapped                 = 200
Regional Root               = 00002.00:A0:00:01:09:0B
RemainingHopCount           = 39
TopChanges                  = 3
================================================================================
Port     |Pri|Prt role|State|PCost     |DCost     |Designated bridge |DPrt
---------+---+--------+-----+----------+----------+------------------+-------
01/01/02 128 Root     frwrd    200000           0 00000.00A00001090B 128.001
01/01/10 128 Designat frwrd    200000           0 32768.00A012BBBBBB 128.010
```

15. GARP Multicast Registration Protocol (GMRP)

Introduction

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping. GMRP and GARP are industry-standard protocols defined by the IEEE 802.1p.

Feature Overview

GMRP can register and deregister multicast group addresses at the MAC layer throughout the Layer 2 connected network. GMRP is Layer 3 protocol independent, which allows it to support the multicast traffic of any Layer 3 protocol (such as IP, IPX etc.).

GMRP software components run both on the switch and on the host (The switch is not a source for GMRP host software). On the host, GMRP is typically used with IGMP: the host GMRP software generates Layer 2 GMRP versions of the host's Layer 3 IGMP control packets. The switch receives both the Layer 2 GMRP and the Layer 3 IGMP traffic from the host. The switch uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN.

NOTE

In all cases, you can use IGMP snooping to constrain multicasts at Layer 2 without the need to install or configure software on hosts.

When a host wants to join an IP multicast group, it sends an IGMP join message, which creates a corresponding GMRP join message. When the switch receives the GMRP join message, it adds the port through which the join message was received to the appropriate multicast group. The switch propagates the GMRP join message to all other hosts in the VLAN, one of which is typically the multicast source.

When the source is multicasting to the group, the switch forwards the multicast only to the ports from which it received join messages for the group.

The switch sends periodic GMRP queries. If a host wants to remain in a multicast group, it responds to the query. In this case, the switch does nothing. If a host does not want to remain in the multicast group, it can either send a leave message or not respond to the periodic queries from the switch. If the switch receives a leave message or receives no response from the host for the duration of the leave-all timer, the switch removes the host from the multicast group.

Supported Standards, MIBs and RFCs

Standards

IEEE 802.1Q

IEEE 802.1D

MIBs

IEEE 802.1Q

RFCs

No RFCs are supported by this feature.

Prerequisites

When Link Aggregation is configured, all the multicast traffic is passed on the master port. For more information about Link Aggregation, refer to the Link Aggregation Groups (LAGs) chapter.

Default GMRP Configuration

Table 15-1 shows the default GMRP configuration.

Table 15-1 GMRP Default Configuration

Parameter	Default Value
GMRP global enable state	Disabled
GARP timers	Join time: 200 ms Leave time: 600 ms Leave all time: 10,000 ms

Configuring and Displaying GMRP

Table 15-2 lists the GMRP commands.

Table 15-2 GMRP Commands

Command	Description
show gmrp	Displays GMRP status.
gmrp	Changes the GMRP status.

Displaying the GMRP Status

The **gmrp** command, in Protocol Configuration mode, and the equivalent **show gmrp** command in Privileged (Enable) mode, display the current GMRP status of the switch, **enabled** or **disabled**.

Command Syntax

```
device-name(cfg protocol)#gmrp
device-name#show gmrp
```

Example 1

```
device-name(cfg protocol)#gmrp
GMRP enabled
```

Example 2

```
device-name#show gmrp
GMRP enabled
```

Changing the GMRP Status

The **gmrp** command, in Protocol Configuration mode, changes the switch's GMRP status to **enable** or **disable**.

By default, GMRP is disabled.

NOTE

1. You must enable GVRP before enabling the GMRP.
2. You must define the system VLAN range before enabling the GMRP.

Command Syntax

```
device-name(cfg protocol)#gmrp {enable | disable}
```

Argument Description

enable	Enable GMRP.
disable	Disable GMRP.

Example

```
device-name(config)#protocol
device-name(cfg protocol)#gmrp enable
device-name(cfg protocol)#end
device-name#show gmrp
GMRP enabled
```

Related Commands

The table below shows the GMRP-related commands.

Table 15-3 GMRP-Related Commands

Command	Description	Described in
garp timer	Sets the GARP timer values.	GVRP (GARP VLAN Registration Protocol) chapter, Description of Commands section
show garp timer	Displays the GARP timer configuration.	GVRP (GARP VLAN Registration Protocol) chapter, Description of Commands section

16. GARP VLAN Registration Protocol (GVRP)

Introduction

GVRP (GARP VLAN Registration Protocol) is part of the IEEE 802.1Q standard for Virtual Bridged LANs, sponsored by the LAN MAN standards Committee of the IEEE Computer Society. The GVRP protocol allows a LAN device to notify neighbors that it is prepared to receive packets for one or more VLANs. The main purpose of the GVRP is to allow GVRP-aware devices to automatically obtain VLAN information without requiring each device to be manually configured to obtain this information. Network servers can also run GVRP. These servers are usually configured to join several VLANs, and then notify the network switches of the VLANs they want to join. The dynamic VLANs that were learned can be viewed by the command **show vlan dynamic** (For more information, see the Commands to Display the VLAN Configuration section in the VLANs (Virtual LANs) chapter).

Configuring and Displaying GVRP Settings

You can use the following GVRP commands:

Table 16-1 GVRP Commands

Command	Description
gvrp	Displays the GVRP.
show gvrp	Displays the GVRP status.
gvrp enable	Enables GVRP.
gvrp disable	Disables GVRP.
no gvrp	Disables GVRP.

Table 16-2 GVRP-Related Commands

Command	Description
garp timer	Sets the GARP timer values.
show garp timerport gvrp enableport gvrp disable	Displays the GARP timer configuration.Enables GVRP on thespecified port.Disables GVRP on thespecified port.

Description of Commands

gvrp

The **gvrp** command, in Protocol Configuration mode, displays the current GVRP status of the switch, **enabled** or **disabled**.

Command Syntax

```
device-name(cfg protocol)#gvrp
```

Example

```
device-name(cfg protocol)#gvrp
GVRP enabled
```

show gvrp

The **show gvrp** command, in Privileged (Enable) mode, displays the current GVRP status of the switch (**enabled** or **disabled**).

Command Syntax

```
device-name#show gvrp
```

Example

```
device-name#show gvrp
GVRP enabled
```

gvrp enable / disable

The **gvrp enable/disable** command, in Protocol Configuration mode, changes the switch's GVRP status to **enable** or **disable**.

When GVRP is enabled, VLANs are allowed to learn details of neighboring VLANs and to apply self-configuration settings based on the information that is learned.

Command Syntax

```
device-name(cfg protocol)#gvrp {enable|disable}
```

Example

```
device-name(config)#protocol
device-name(cfg protocol)#gvrp  enable
Only the first 64 vlans will be saved, proceed? [y/n] : y
device-name(cfg protocol)#gvrp
GVRP enabled
```

The message that appears on the screen reports the number of VLANs that the switch can support. The ESB26 is limited to 64 VLANs.

To enable GVRP, enter **y** (otherwise, GVRP will not be enabled).

no gvrp

The **no gvrp** command, in Protocol Configuration mode, changes the switch's GVRP status to **disable**. This command is equivalent to **gvrp disable**.

Command Syntax

```
device-name(cfg protocol)#no gvrp
```

garp timer

The **garp timer** command, in Protocol Configuration mode, sets the GARP timer values. The **no** form of this command resets the specified timer to its default vallue if possible (see the <300-20000> argument parameter described below). The **no** form of this command used without parameters resets all timers to their default vallues.

Command Syntax

```
device-name(cfg protocol)#garp timer {leave|leaveall} <300-20000>
device-name(cfg protocol)#garp timer {join} <100-6666>
device-name(cfg protocol)#no garp timer {join|leave|leaveall}
device-name(cfg protocol)#no garp timer
```

Argument Description

join	GARP Join timer.
leave	GARP Leave timer.
leaveall	GARP LeaveAll timer.
<300-20000> **<100-6666>**	Refresh interval for the specified timer. The **leave** timer refresh interval must be equal to or smaller than the **leaveall** timer refresh interval. The **join** timer refresh interval must be no grater than one-third of the **leave** timer refresh intervall.

Example

```
device-name(cfg protocol)#garp timer join 200
GARP Join timer value is 200 milliseconds
device-name(cfg protocol)#
```

show garp timer

The **show garp timer** command, in Privileged (Enable) mode, displays the current status of the GARP timers.

Command Syntax

```
device-name#show garp timer
```

Example

```
device-name#show garp timer
GARP enabled
================================
 Timer    | Value (milliseconds)
--------------------------------
 Join             200
 Leave            600
 LeaveAll       10000
device-name#
```

port gvrp enable / disable

The **port gvrp enable/disable** command, in Interface Configuration mode, changes the port GVRP status to **enable** or **disable**, respectively. Disabling GVRP on a port will disable GVRP packets transmit from that port.

Command Syntax

```
device-name(config-if 1/1/1)#port gvrp {enable|disable}
```

17. Virtual LANs (VLANs)

Introduction

A VLAN is a logical collection of endpoint devices, typically referred to as either clients or servers that can be located anywhere in a network, but communicate as if they were on the same physical segment. Segments are flexible user groups that you create with the command-line interface.

Benefits of using VLANs

Using VLANs on your networks provides the following advantages over traditional networks: **flexibility**, **security** and **better control** of broadcast traffic.

- Flexibility – In traditional networks, when users are moved physically to different subnets, administrators need to spend much time in updating the IP address of each end-station. This is not required in VLANs.
- Security - devices within a VLAN can communicate directly only with devices in the same VLAN. Communication between devices in different VLANs must pass through a routing device or Layer 3 switch.
- Better control of broadcast traffic - Traditional networks may become congested by broadcast traffic that is directed to all network devices, whether or not they require it. With VLANs, you can increase the efficiency of your network by configuring each VLAN to contain only devices that must communicate with each other.

VLAN Types

VLANs can be configured according to the following criteria:

- Physical port
- 802.1Q tag
- MAC address
- A combination of the above criteria

Port-Based VLANs

A port-based VLAN is a group of switch ports designated by the switch as belonging to the same broadcast domain. In a port-based VLAN, a VLAN name is given to a group of one or more ports on the switch. While in older switches, a port can be a member of only one port-

based VLAN, BiNOS follows the 802.1Q standard that lets you assign a single switch port to two or more VLANs.

Tagging VLANs

Tagging is a process that inserts a marker (called a tag) into the Ethernet frame. The tag contains the identification number of a specific VLAN, called the VLAN ID.

The use of 802.1Q tagged packets may lead to the appearance of packets slightly bigger than the current IEEE 802.3/Ethernet maximum of 1,518 bytes. This may affect packet error counters in other devices, and may also lead to connectivity problems if non-802.1Q bridges or switches are placed in the path. By default all the interfaces in the device belong to VLAN tag number 1 (the VLAN name is *default*).

Port Default VLAN

In Port-based VLAN classification within a switch, the VLAN ID associated with an untagged or priority-tagged frame (i.e., a frame with no tag header, or a frame with a tag header that carries the null VLAN ID) is determined, based on the Port of arrival of the frame into the Switch. This classification mechanism requires the association of a specific VLAN ID, the *Port VLAN Identifier*, or *PVID*, with each of the Switch's Ports. The PVID is also known as the port's *default VLAN*.

The PVID for a given port provides the VID for untagged and priority-tagged frames received through that port. The PVID for each port contains a valid VID value, not the value of the null VLAN ID.

If no PVID value has been explicitly configured for a port, the PVID assumes the value of the default PVID=1. This will result that even though a port is added to a certain VLAN, untagged traffic will not flow on that VLAN until the port's default VLAN is set to that VLAN.

NOTE

A port can be configured for more than one untagged VLAN, but with only one PVID. If a port is a member of several VLANs, its PVID can be changed with the default vlan command in Interface Configuration mode, or with the add ports default command in a specific VLAN Configuration mode.

Uses of Tagged VLANs

Tagging is most commonly used to create VLANs that span switches; an example of this type of VLAN is shown in Figure 17-1.

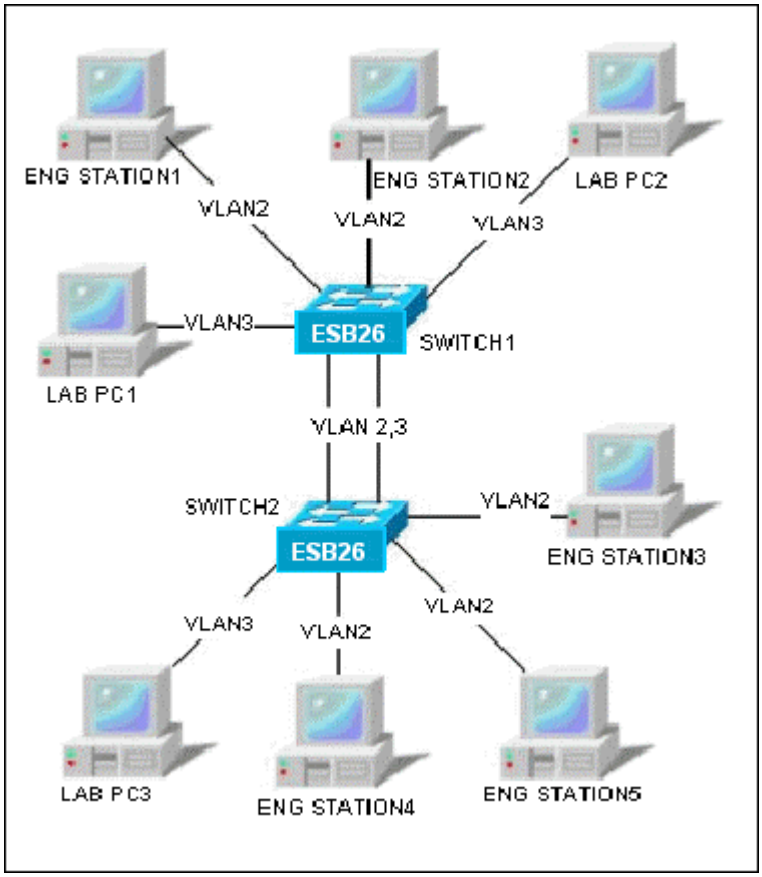


Figure 17-1 VLAN Spanning Two Switches

The switch-to-switch connections are typically called trunks. Using tags, multiple VLANs can span multiple switches using one or more trunks. In a port-based VLAN, each VLAN requires its own pair of trunk ports. Using tags, multiple VLANs can span two switches with a single trunk. Another benefit of tagged VLANs is the ability to use multiple VLANs through one port. This is particularly useful if you have a device (such as a server), that must belong to multiple VLANs. The device must have a NIC that supports 802.1Q tagging.

Assigning a VLAN Tag

Each VLAN may be assigned an 802.1Q VLAN tag. As ports are added to a VLAN with an 802.1Q tag defined, you need to decide whether each port will have tagging assigned for that VLAN.

The default mode of the switch is to have all ports assigned to the default VLAN that has the name *default* and an 802.1Q VLAN tag (VLAN ID) of 1.

Not all ports in the VLAN must be tagged. As traffic from a port is forwarded out of the switch, the switch determines (in real time) if each destination port should use tagged or untagged packet formats for that VLAN. The switch adds and strips tags, as required, by the port configuration for that VLAN. Packets arriving tagged with a VLAN ID that is not configured on a port will be discarded.

Description of Commands

Commands to Display the VLAN Configuration

Figure 17-1 summarizes the commands available for displaying the VLANs. You can use the **show** command (with no arguments) in the general VLAN configuration mode or in a specific VLAN configuration mode to display the VLAN configuration. The other commands summarized in the table are available in Privileged (Enable) mode.

Table 17-1 Commands for displaying the VLANs

Command	Description
show	Displays the VLAN configuration (this command is available in the general VLAN configuration mode and in any specific VLAN configuration mode).
show vlan	Displays the VLANs configuration.
show vlan dynamic	Displays the dynamic VLANs.
show vlan management	Displays the management VLANs.

show vlan

The **show vlan** command, in Privileged (Enable) mode, displays information regarding the VLANs defined in the system. The command is equivalent to the **show** command in VLAN Configuration mode.

Command Syntax

```
device-name#show vlan
```

Example

```
device-name#show vlan
================================================================================
 Name                |VTag| Tagged ports         | Untagged ports
--------------------+----+----------------------+--------------------
default              |1   |                      |1/1/1-1/1/2
```

show

The **show** command, in Global and Specific VLAN Configuration modes, displays information regarding the VLANs defined in the system. The command is equivalent to the **show vlan** command in View and Privileged (Enable) mode.

Command Syntax

```
device-name(config vlan)#show
```

show vlan dynamic

The **show vlan dynamic** command, in Privileged (Enable) mode, displays information regarding the dynamic VLANs learned by the GVRP.

Command Syntax

```
device-name#show vlan dynamic
```

Commands to Configure VLAN Settings

BiNOS allows you to configure 802.1Q-compatible VLANs. Compatibility with the 802.1Q standard lets you assign a single switch port to two or more VLANs, while still allowing for interfacing with older switches that require a separate port for each VLAN.

An example of three VLANs on one switch is shown in Figure 17-2.

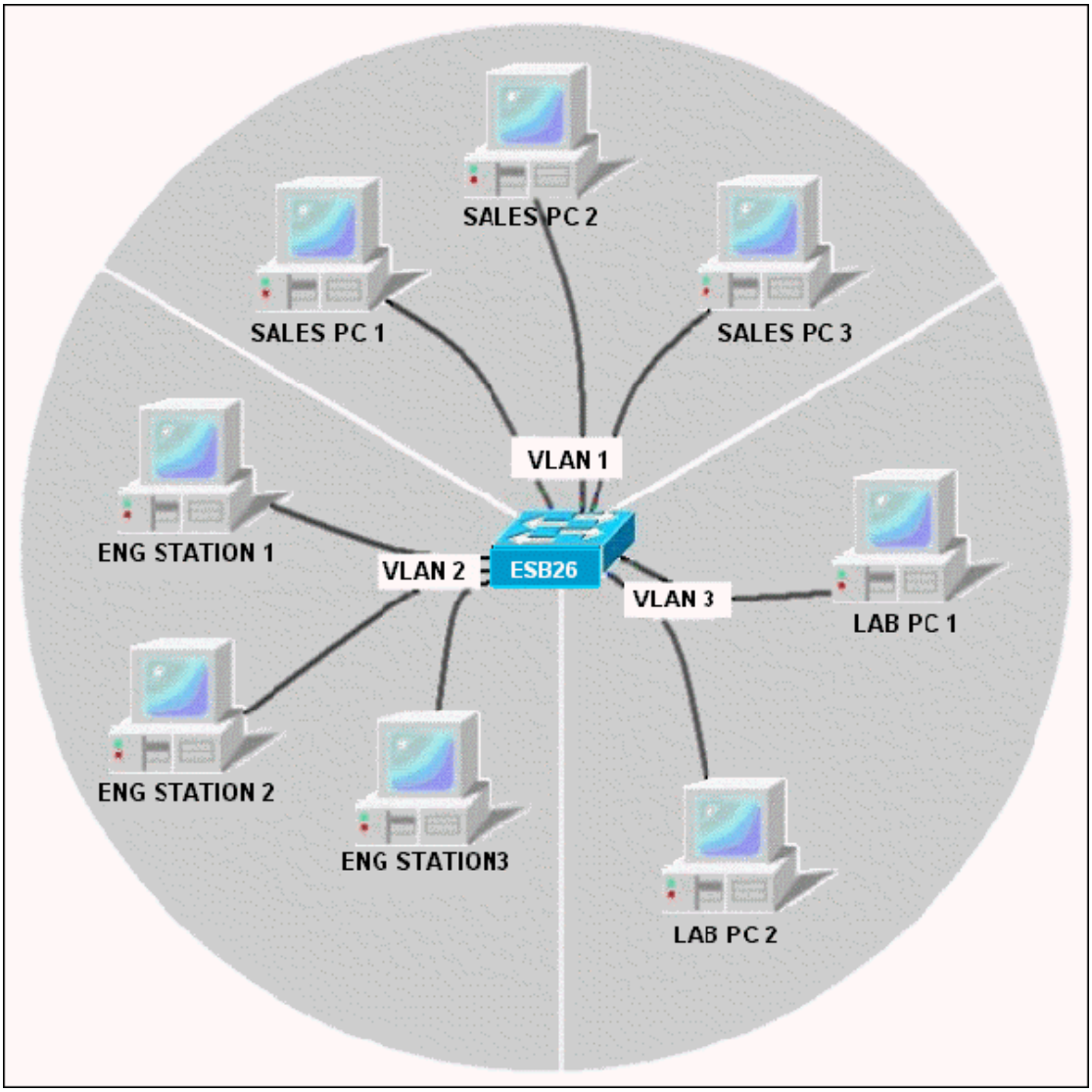


Figure 17-2 Three VLANs on One Switch

In port-based VLAN classification within a switch, the VLAN ID associated with an untagged or priority-tagged frame (i.e., a frame without a tag header, or with a tag header that carries the null VLAN ID) is determined, based on the frame's port of arrival into the switch. This classification mechanism requires the association of a specific VLAN ID, the *Port VLAN Identifier*, or *PVID*, with each of the switch's ports.

The PVID for a given port provides the VID for untagged and priority-tagged frames received through that port. The PVID for each port contains a valid VID value, not the value of the null VLAN ID.

If no PVID value has been explicitly configured for a Port, the PVID assumes the value of the default PVID=1.

You can create, delete and display VLANs in the global VLAN Configuration mode. You can configure a specific VLAN in the specific global VLAN Configuration mode. To access a specific VLAN configuration mode, use the **config** command in the global VLAN Configuration mode.

Table 17-2 summarizes the commands that are available in the global VLAN Configuration mode.

Table 17-2 Commands in Global VLAN Configuration Mode

Command	Description
create	Creates a VLAN with specified name and tag number.
delete	Deletes the VLAN specified by its name.
delete-id	Deletes the VLAN specified by its VLAN id.
show	Shows information regarding all existing VLANs.
create range	Creates VLANs by sequence
delete range	Deletes VLANs by sequence
config	Accesses a specific VLAN configuration mode.
management	Controls access to switch management on specified VLANs.

Table 17-3 summarizes the commands that are available in a specific VLAN Configuration mode.

Table 17-3 Commands in Specific VLAN Configuration Mode

Command	Description
add ports	Adds ports to VLAN
add ports default	Sets PVID of specified port(s)
remove ports	Removes ports from VLAN
remove ports default	Removes PVID of specified port(s)
config	Switches Configuration mode to another VLAN.
show	Shows all VLAN configurations

Table 17-4 summarizes the commands that are available in the global Configuration mode.

Table 17-4 Commands in Global Configuration Mode

Command	Description
vlan	Changes the mode from the global Configuration to VLAN Configuration mode.

vlan

The **vlan** command, in Global Configuration mode, changes the mode from the global Configuration to VLAN Configuration mode. VLAN Configuration mode provides access to VLAN Configuration commands.

Command Syntax

```
device-name(config)#vlan
device-name(config vlan)#
```

create

The **create** command, in VLAN Configuration mode, creates a VLAN with the specified name and tag (VLAN serial number).

Command Syntax

```
device-name(config vlan)#create NAME <vlan-id>
```

Argument Description

NAME	VLAN name.
vlan-id	VLAN tag number, in the range <2-4094>

Example

```
device-name(config vlan)#create accounting 2
```

This example creates a VLAN named ***accounting*** with tag number 2.

delete

The **delete** command, in VLAN Configuration mode, deletes the VLAN specified by its VLAN name.

Command Syntax

```
device-name(config vlan)#delete NAME
```

Argument Description

NAME	VLAN name of an existing VLAN.

Example

```
device-name(config vlan)#delete accounting
```

This example deletes the VLAN named ***accounting***.

delete id

The **delete id** command, in VLAN Configuration mode, deletes the VLAN specified by its VLAN ID.

Command Syntax

```
device-name(config vlan)#delete id <vlan-id>
```

Argument Description

vlan-id	Represents the ID number of an existing VLAN (2- 4094)

Example

```
device-name(config vlan)#delete id 10
```

This example deletes the VLAN with id 10

create range

The **create range** command, in VLAN Configuration mode, creates a sequence of VLANs in the specified tag-number range, and automatically assigns VLAN names that match the tag-numbers.

With the **create range** command you can also add specified port(s) as either tagged or untagged ports.

The VLAN name that is automatically assigned is of the form **Vlan_*dddd***, where ***dddd*** represents a 1-to-4 digit number equal to the matching tag number. For example, the VLAN created with tag-number 123 gets the name **Vlan_123**.

Command Syntax

```
device-name(config vlan)#create range <vlan-id1> <vlan-id2> [PORTLIST tagged [PORT-LIST untagged]]
device-name(config vlan)#create range <vlan-id1> <vlan-id2> [PORTLIST untagged [PORT-LIST tagged]]
```

Argument Description

vlan-id1	Beginning of range, <2-4094>. Must be less than vlan-id2.
vlan-id2	End of range, <2-4094>. Must be greater than vlan-id1.
PORT-LIST	(Optional) One or more port numbers, specified by the following options: UU/SS/PP – (unit, slot and port number), e.g. – 1/1/8 specifying a single port;

	UU – (1 or 2-digit unit number) specifying all ports on unit; UU/SS – (unit and slot number) specifying all ports on slot; A hyphenated range of ports, e.g. - 1/1/9-1/1/16 or 1/2-1/3. Several port numbers and/or ranges, separated by commas, e.g. 1/1, 1/1/3-1/1/6, 1/1/8.
tagged	(Optional) Specifies that the ports are tagged on the specified ports.
untagged	(Optional) Specifies that the ports are untagged on the specified ports.

NOTE

You can only specify ports that are all tagged or all untagged. For a "mixed" configuration, you can add ports of either kind with the add ports command in each specific VLAN's configuration mode.

In the PORT-LIST, blank spaces before or after the comma that separates sequential lists are not allowed.

Example

```
device-name(config vlan)#create range 15 20 1/1/1-1/1/3 untagged
```

This example creates a sequence of VLANs that you can display as follows:

```
device-name(config vlan)#show
================================================================================
 Name                |VTag| Tagged ports         | Untagged ports
--------------------+----+----------------------+---------------
default              |1   |                      |1/1/1-1/1/26
Vlan_15              |15  |                      |1/1/1-1/1/3
Vlan_16              |16  |                      |1/1/1-1/1/3
Vlan_17              |17  |                      |1/1/1-1/1/3
Vlan_18              |18  |                      |1/1/1-1/1/3
Vlan_19              |19  |                      |1/1/1-1/1/3
Vlan_20              |20  |                      |1/1/1-1/1/3
```

delete range

The **delete range** command, in VLAN Configuration mode, deletes a sequence of VLANs in the specified tag-number range.

Command Syntax

```
device-name(config vlan)#delete range <vlan-id1> <vlan-id2>
```

Argument Description

vlan-id1	Beginning of range, <2-4094>. Must be less than vlan-id2.
vlan-id2	End of range, <2-4094>. Must be greater than vlan-id1.

Example

```
device-name(config vlan)#delete range 15 18
device-name(config vlan)#show
```

```
=====================================================================
 Name               |VTag| Tagged ports         | Untagged ports
--------------------+----+----------------------+---------------
default             |1   |                      |1/1/1-1/1/26
Vlan_19             |19  |                      |1/1/1-1/1/3
Vlan_20             |20  |                      |1/1/1-1/1/3
```

config

The **config** command, in VLAN Configuration mode, changes the mode to Configuration mode of a specific VLAN. You can also use this command in a specific VLAN Configuration mode to switch the Configuration mode to another specific VLAN.

Commands available in a specific VLAN Configuration mode are listed in Table 17-3. These commands are described below.

Command Syntax

```
device-name(config vlan)#config NAME1
device-name(config-vlan NAME1)#config NAME2
```

Argument Description

NAME1, NAME2	Represent the names of existing VLANs

Examples

1. Changing from the global VLAN configuration mode to a specific VLAN Configuration mode, as indicated by the prompt-line that follows:

```
device-name(config vlan)#config vlan_52
device-name(config-vlan vlan_52)#
```

2. Switching the configuration mode from one specific VLAN to another, as indicated by the prompt-line that follows:

```
device-name(config-vlan vlan_52)#config XYZ
device-name(config-vlan XYZ)#
```

add ports

The **add ports** command, in Specific VLAN Configuration mode, adds the specified port(s) as either tagged or untagged ports. The command assigns the port the ability to handle the VLAN tagging in the Ethernet packet in ingress and egress. Tagged ports look for a VLAN tag that is assigned in ingress packets. In egress packets, the VLAN is assigned to the packet according to the configuration.

Command Syntax

```
device-name(config-vlan VLAN-NAME)#add ports PORT-LIST {tagged|untagged}
```

Argument Description

PORT-LIST	One or more port numbers, specified by the following options: • UU/SS/PP – (unit, slot and port number), e.g. – 1/1/8 specifying a single port;

- UU – (1 or 2-digit unit number) specifying all ports on unit;
- UU/SS – (unit and slot number) specifying all ports on slot;
- A hyphenated range of ports, e.g. - 1/1/9-1/1/16;
- Several port numbers and/or ranges, separated by commas, e.g. – 1/1/1, 1/1/3-1/1/6, 1/1/8.

tagged Specifies that the ports are tagged.

untagged Specifies that the ports are untagged.

NOTES

1. A single usage of the add ports command allows you to only specify ports that are all tagged or all untagged. For a "mixed" configuration, you can apply this command more than once. See also the create range global VLAN configuration command.
2. In the PORT-LIST, blank spaces before or after the comma that separates sequential lists are not allowed.

Example

The following example adds four untagged ports and three tagged ports to the VLAN that has the name xxx, and already has previous ports 1/1/1 and 1/1/12-1/1/15 configured to it. The result is displayed by the **show** command that can be applied in any specific or global VLAN Configuration mode.

```
device-name(config-vlan xxx)#add ports 1/1/2-1/1/5 untagged
device-name(config-vlan xxx)#add ports 1/1/8-1/1/9,1/1/12 tagged
device-name(config-vlan xxx)#show
=================================================================
 Name         |VTag          | Tagged ports         | Untagged ports
--------------+--------------+----------------------+---------------
default       |1             |                      |1/1/1-1/1/26
xxx           |9             |1/1/1,1/1/8,1/1/9,    |1/1/2-1/1/5
              |              |1/1/12-1/1/15         |
```

add ports default

The **add ports default** command, in Specific VLAN Configuration mode, assigns the VLAN ID of the configured VLAN as the PVID (port's default VLAN) of one or more specified ports.

Command Syntax

```
device-name(config-vlan VLAN-NAME)#add ports default PORT-LIST
```

Argument Description

PORT-LIST One or more port numbers, specified by the following options:

- UU/SS/PP – (unit, slot and port number), e.g. – 1/1/8 specifying a single port;
- UU – (1 or 2-digit unit number) specifying all ports on unit;
- UU/SS – (unit and slot number) specifying all ports on slot;
- A hyphenated range of ports, e.g. - 1/1/9-1/1/16.
- Several port numbers and/or ranges, separated by commas, e.g. – 1/1/1, 1/1/3-1/1/6, 1/1/8.

Example

The following commands configure port 1/1/1 as an untagged member in vlan_2, vlan_3 and vlan_4, that have VLAN IDs 2, 3 and 4 respectively. The **add ports** command in vlan_3 configuration mode assigns the VLAN ID of vlan_3, (which is 3) as PVID of port 1/1/1.

```
device-name(config vlan)#create range 2 4
device-name(config vlan)#config vlan_2
device-name(config-vlan vlan_2)#add ports 1/1/1-1/1/3 untagged
device-name(config vlan)#config vlan_3
device-name(config-vlan vlan_3)#add ports 1/1/1-1/1/5 untagged
device-name(config-vlan vlan_3)#add ports default 1/1/1
device-name(config vlan)#config vlan_4
device-name(config-vlan vlan_4)#add ports 1/1/1,1/1/5,1/1/7 untagged
device-name(config-vlan vlan_4)#exit
```

remove ports

The **remove ports** command, in Specific VLAN Configuration mode, removes the specified port(s).

Command Syntax

```
device-name(config-vlan VLAN-NAME)#remove ports PORT-LIST
```

Argument Description

PORT-LIST	One or more port numbers, specified by the following options: • UU/SS/PP – (unit, slot and port number), e.g. – 1/1/8 specifying a single port; • UU – (1 or 2-digit unit number) specifying all ports on unit; • UU/SS – (unit and slot number) specifying all ports on slot; • A hyphenated range of ports, e.g. - 1/1/9-1/1/16. • Several port numbers and/or ranges, separated by commas, e.g. – 1/1/1, 1/1/3-1/1/6, 1/1/8.

Example

The following example removes the specified ports from the VLAN that has the name xxx. The result is displayed by the **show** command that can be applied in any specific or global VLAN Configuration mode.

```
device-name(config-vlan xxx)#remove ports 1/1/1-1/1/4,1/1/12
device-name(config-vlan xxx)#show
================================================================
 Name         |VTag          | Tagged ports         | Untagged ports
--------------+--------------+----------------------+---------------
default       |1             |                      |1/1/1-1/1/26
xxx           |9             |1/1/8,1/1/9,          |1/1/5
              |              |1/1/13-1/1/15         |
```

remove ports default

The **remove ports default** command, in Specific VLAN Configuration mode, removes the PVID (port's default VLAN) from one or more specified ports. The ports PVID is restored to the default VLAN (VLAN ID 1).

Command Syntax

```
device-name(config-vlan VLAN-NAME)#remove ports default PORT-LIST
```

config-dynamic

The **config-dynamic** command, in VLAN Configuration mode, changes the mode to configuration mode of a specific dynamic VLAN to static mode. You can also use this command in a specific VLAN Configuration mode. This command will switch the Configuration mode to the new VLAN configuration mode.

The **config-dynamic** command allows entering the VLAN configuration mode of a specific VLAN for dynamic GVRP VLAN by converting the dynamic GVRP VLAN to static VLAN.

Once entering the VLAN configuration mode of a specific VLAN, this VLAN becomes static and gets the system name *Dynamic_<vid>* (e.g. Dynamic_2).

The VLAN's dynamic interfaces can be shown with the **show vlan dynamic** command and the VLAN's static interfaces can be shown with the **show vlan** command.

To delete the converted VLAN, use the **delete** commands for the static VLANs (disabling the GVRP won't erase the converted VLANs).

Command Syntax

```
device-name(config vlan)#config-dynamic <vlan-id>
```

Argument Description

vlan-id	Specifies the VLAN ID number, in the range <2-4094>.

Example

Configuring the dynamic GVRP VLAN 2:

```
device-name(config vlan)#config-dynamic 2
device-name(config-vlan Dynamic_2)#
```

management

The **management** command, in VLAN Configuration mode, provides access to the switch's management on the specified VLANs. The **no** form of this command blocks access to the switch's management on the specified VLANs.

By default, management of the switch is accessible on all VLANs.

Use the **management** command to limit switch management access to VLANs that you specify by a list of VLAN ID numbers. You may include VLANs that have not been created yet and VLANs that were dynamically learned by the GVRP.

Before applying the **management** command, verify that the following conditions are met:

- You must be able to move your network management station to a switch port assigned to the same VLAN as the management VLAN.
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.

If VLAN management is disabled, the following will be disallowed:

- Telnet to the switch
- SSH to the switch
- SNMP management
- Ping to the switch
- TFTP download or upload

Command Syntax

```
device-name(config vlan)#management VLAN-list
```

Argument Description

VLAN-list	List of VLAN IDs, in the form {k|k1-k2} [, {l | l1-l2}[,{m|m1-m2}[,…]]], where commas are used as term separators and hyphenated terms represent ranges. For example: The expression 2,4,8-32,64-512 represents VLAN IDs 2, 4, the range from 8 to 32 and the range from 64 to 512.

Example

In the following example, the switch can be managed only by VLAN 2. VLAN 100, 101 and 102 were created but the switch cannot be managed from the workstations, only from the management station.

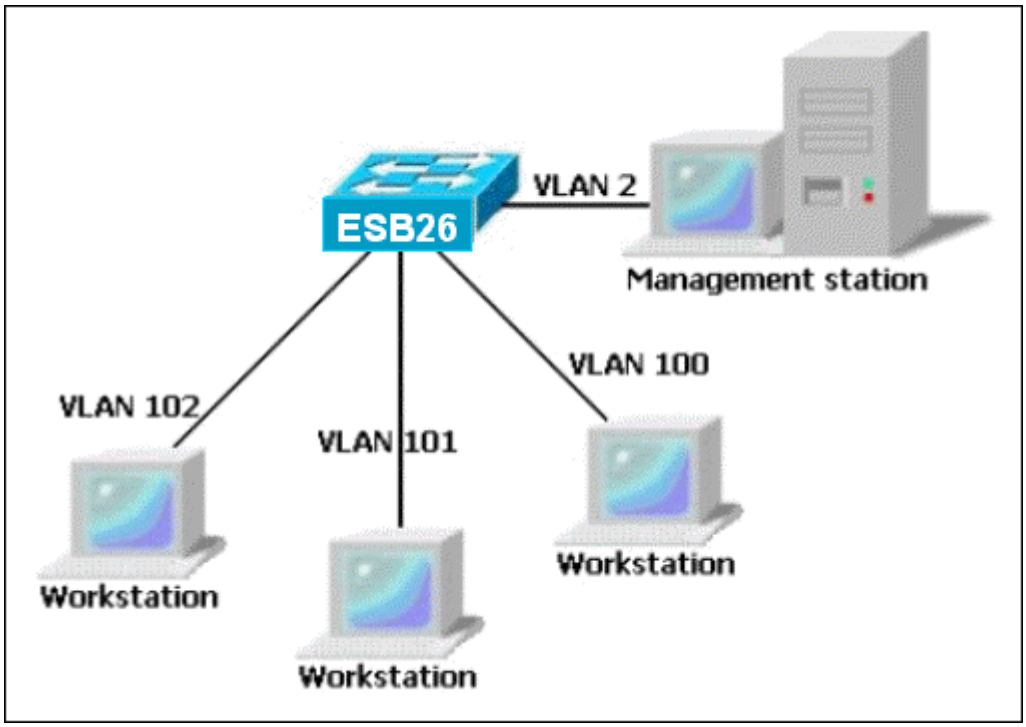


Figure 17-3 VLAN Management Example

```
device-name#configure terminal
```

```
device-name(config)#vlan
device-name(config vlan)#no management 1,3-4094
device-name(config vlan)#create manage 2
device-name(config vlan)#config manage
device-name(config-vlan manage)#add ports 1/1/2 untagged
device-name(config-vlan manage)#add ports default 1/1/2
device-name(config-vlan manage)#exit
device-name(config vlan)#create v100 100
device-name(config vlan)#config v100
device-name(config-vlan v100)#add ports 1/1/3 untagged
device-name(config-vlan v100)#add ports default 1/1/3
device-name(config-vlan v100)#add ports 1/1/10 tagged
device-name(config-vlan v100)#exit
device-name(config vlan)#create v101 101
device-name(config vlan)#config v101
device-name(config-vlan v101)#add ports 1/1/11 untagged
device-name(config-vlan v101)#add ports default 1/1/11
device-name(config-vlan v101)#add ports 1/1/12 tagged
device-name(config-vlan v101)#exit
device-name(config vlan)#create v102 102
device-name(config vlan)#config v102
device-name(config-vlan v102)#add ports 1/1/4 untagged
device-name(config-vlan v102)#add ports default 1/1/4
device-name(config-vlan v102)#add ports 1/1/13 tagged
device-name(config-vlan v102)#exit
device-name(config vlan)#config default
device-name(config-vlan default)#remove ports 1/1/2-1/1/4,1/1/13
device-name(config-vlan default)#exit
```

show vlan management

The **show vlan management** command, in Privileged (Enable) mode, displays which VLANs provide management access.

Command Syntax

```
device-name#show vlan management
```

Example

The following example shows that by default, management is accessible on all VLANs. After we apply the **no management** command to block access on a specified list of VLANs, the response to the **show vlan management** command indicates that management is accessible only on VLANs in the complementary list.

```
device-name#show vlan management
Management VLANs: 1-4094
device-name(config)#vlan
device-name(config vlan)#no management 1,5-7,21-4093
...
device-name#show vlan management
Management VLANs: 2-4,8-20,4094
device-name#
```

18. Quality of Service

Introduction

Today's networks transmit data streams for various applications using many different protocols. Different types of traffic sharing a data path through the network can interact in ways that affect their application performance. Traffic prioritization becomes especially important when delay-sensitive, interactive applications are supported across the network. In many cases a guaranteed level of throughput is part of contractual obligations between the network operator and customers or third-party service providers.

Policy-based Quality of Service (QoS) allows you to specify different service levels for traffic traversing the switch. Policy-based QoS is an effective control mechanism for networks that have heterogeneous traffic patterns. Using Policy-based QoS, you can specify the service level for a traffic type or host.

QoS controls congestion by determining the order in which packets are transmitted based on priorities assigned to those packets. QoS queuing policies can protect bandwidth for important categories of applications, or specifically limit the bandwidth associated with less critical traffic. For example, if Voice Over IP (VOIP) traffic requires a reserved amount of bandwidth to function properly, QoS policies can reserve sufficient bandwidth for this type of application. Other applications deemed less critical can be limited in their bandwidth usage.

During periods of light traffic, QoS policies have little effect, and packets are transmitted as soon as they arrive. During periods of congestion, outbound packets accumulating at an interface are sorted into eight queues. They are transmitted from the queues according to the queuing mechanism configured for the interface.

Feature Overview

When using QoS feature, each physical port sorts inbound and outbound traffic into eight queues for the QoS processing.

You control Quality of Service behavior in two ways:

By configuring the criteria used to sort inbound and outbound packets into the eight queues. By default, values of the 802.1p priority field of the packet header are mapped to the eight QoS queues. You can also map destination MAC address priority values to the QoS queues.

By selecting the queuing mechanism to apply to the outbound queues. Two basic queuing mechanisms are provided:

- **Weighted Round-Robin** queuing lets you assign a relative weight to each queue, which determines the bandwidth assigned to each queue relative to the others.
- **Strict Priority** queuing sets the eight queues in a rigid order, and always transmits packets from the highest-priority queue that has packets waiting.

In addition, two hybrid queuing schemes are available, which combine the Weighted Round Robin and Strict Priority mechanisms.

Traffic Analysis for QoS Deployment

To effectively configure QoS, you must analyze the types of traffic using the interface and determine their relative bandwidth demands. You should also evaluate the supported applications' sensitivity to latency, jitter, and packet loss.

General guidelines for each traffic type are given below. Consider them as general guidelines and not strict recommendations. Once QoS parameters are set, you can monitor the performance of the application to determine if the actual behavior of the applications matches your expectations.

- ***Voice*** applications demand small amounts of bandwidth. However, the bandwidth must be constant and predictable because voice applications are typically sensitive to latency (inter-packet delay) and jitter (variation in inter-packet delay).
- ***Video*** applications are similar in needs to voice applications, with the exception that bandwidth requirements are somewhat larger, depending on the encoding.

  It is important to understand the behavior of the video application being used. Some applications can transmit large amounts of data for multiple streams in one "spike," with the expectation that the end-stations will buffer significant amounts of video-stream data. This can present a problem to the network infrastructure, because it must be capable of buffering the transmitted spikes where there are speed differences (for example, going from Gigabit Ethernet to Fast Ethernet).
- ***Database*** applications such as those associated with ERP, typically do not demand significant bandwidth and are tolerant of delay. You can establish a minimum bandwidth using a priority less than that of delay-sensitive applications.
- ***Web browsing*** applications cannot be generalized into a single category. Casual and application-oriented traffic can be distinguished from each other by their server source and destinations.

Most browser-based applications have an asymmetric dataflow (small dataflows from the browser client, large dataflows from the server to the browser client). An exception to this pattern may be created by some Java™ -based applications.

Web-based applications are generally tolerant of latency, jitter, and some packet loss, but small packet-loss may have a large impact on perceived performance due to the nature of TCP.

File server applications typically pose the greatest demand on bandwidth, although they are very tolerant of latency, jitter, and some packet loss, depending on the network operating system and the use of TCP or UDP.

Sorting Packets for QoS Handling

Packet Sorting by 802.1p Priority Values

Nokia ESB26 supports the standard 802.1p priority bits that are part of a tagged Ethernet packet. The 802.1p bits can be used to prioritize the packet.

When a packet arrives at the switch, the switch examines the 802.1p priority field and assigns the packet to a specific QoS queue for transmission. The 802.1p priority field is located directly following the 802.1Q type field, and preceding the 802.1Q VLAN ID, as shown in Figure 18-1.

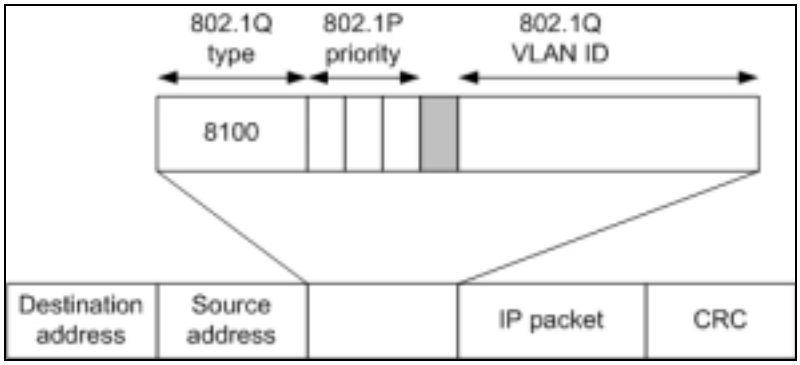


Figure 18-1 802.1p Priority Header Fields

When the switch detects ingress traffic that contains 802.1p prioritization information, the traffic is mapped to various hardware queues on the egress port of the switch. The transmitting hardware queue determines the bandwidth management and priority characteristics used when transmitting packets.

The default mapping of each 802.1p priority value to QoS priority is shown in table 18-2. To change the default configuration use the command **qos map** command in Global Configuration mode.

By default, 802.1p priority information is not replaced or manipulated, and the information observed on ingress is preserved when the packet is transmitted. This behavior is not affected by the switching or routing configuration of the switch. However, the switch is capable of inserting and/or overwriting 802.1p priority information when it transmits an 802.1Q tagged frame. The 802.1p priority information that is transmitted is determined by the hardware queue that is used when transmitting the packet. To replace 802.1p priority information, use the **qos remark** command in Global Configuration mode.

NOTE The switch does not change the VLAN Priority Tag (VPT) for a switched packet that comes with an 802.1Q tag, since it assumes that the sender of the packet has already determined the VPT.

Packets received without a tag have their VPT set in by the command qos remark.

MAC-Based Traffic Groupings

QoS priority values can be assigned to packets destined for a specific MAC address.

The MAC address options, defined below, are as follows:

- For static and secured MAC addresses, this can be done by using the **qos mac** command in Global Configuration mode. This command creates a static MAC address with the specified priority.
- For dynamic MAC addresses, the MAC address inherits the priority from the port on which it was learned.

The priority on the port is configured by the **qos priority** command in Interface Configuration mode.

NOTE When changing the priority on the port the priority of the dynamic MAC address is also changes.

Traffic Scheduling

Congestion management features allow you to control congestion by determining the order in which packets are transmitted based on priorities assigned to those packets. Congestion management entails the creation of queues, assignment of packets to those queues based on the packet's classification, and scheduling of the packets in a queue for transmission. If you use congestion management features, packets accumulating at an interface are queued until the interface is free to transmit them; they are then scheduled for transmission according to their assigned priority and the queuing mechanism configured for the interface. The determines the order of packet transmission by controlling which packets are placed in which queue and how queues are serviced with respect to each other.

First-In, First-Out Queuing

In FIFO queuing, also known as first-come, first-served (FCFS) queuing, packets are queued when the network is congested, and forwarded in order of arrival when the network is no longer congested.

FIFO applies no prioritization or classification of traffic and. There is only one queue, and all packets are treated equally. Packets are sent out in the order in which they arrive. Higher priority packets are not transmitted faster than lower priority packets.

When FIFO is used, ill-behaved sources can consume all the bandwidth, bursty sources can cause delays in time-sensitive or important traffic, and important traffic can be dropped because less important traffic fills the queue.

Strict Priority (SP)

With Strict Priority (SP) queue handling, the queues are ranked in order. The highest ranking queue *txq7* is serviced first until it is empty, then the lower queues *txq6*, *txq5*, *txq4, txq3*, *txq2*, *txq1* and *txq0* are serviced in sequence. SP provides absolute preferential treatment to high priority traffic, ensuring that mission-critical traffic traversing various WAN links gets priority treatment. In addition, SP provides a faster response time than do other methods of queuing.

Use the SP mechanism to guarantee a fixed portion of available bandwidth to one type of application - for example, interactive multimedia applications - possibly at the expense of less critical traffic. But when you choose to use SP, consider that lower priority traffic is often denied bandwidth in favor of higher priority traffic, so use of SP could, in the worst case, result in lower priority traffic never being transmitted. To avoid inflicting these conditions on lower priority traffic, you can use rate-limit to control the rate of the higher priority traffic. Figure 18-2 illustrates the SP process.

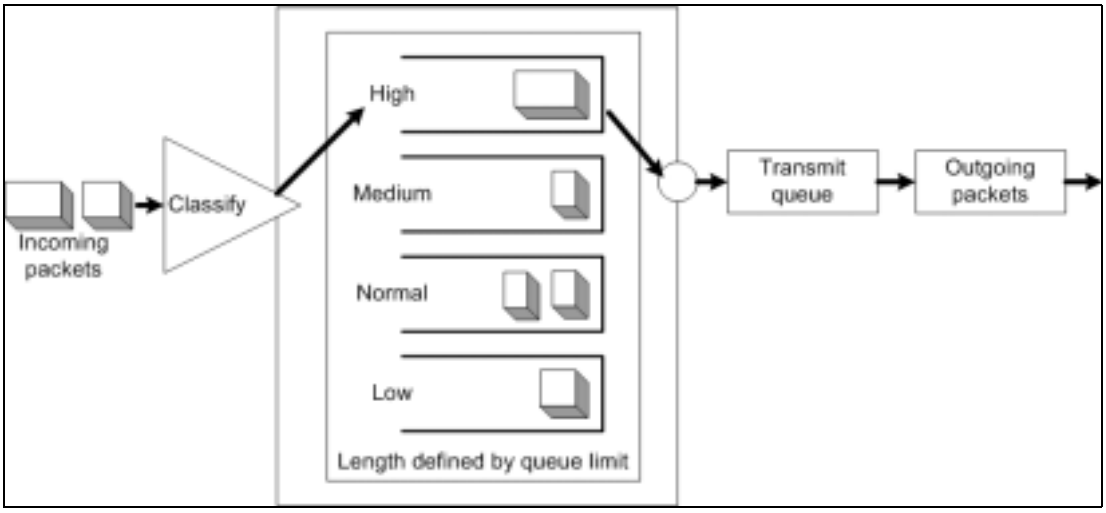


Figure 18-2 Strict Priority Queuing

Benefits of SP Queuing

SP provides absolute preferential treatment to high priority traffic, ensuring that mission-critical traffic traversing various WAN links gets priority treatment. In addition, SP provides a faster response time than do other methods of queuing.

Weighted Round Robin (WRR)

In this scheduling method, a weighting factor for each queue determines how many bytes of data the system delivers from the queue before it moves on to the next queue. The WRR mechanism is cycles through the queues. For each queue, packets are sent until the number of bytes transmitted exceeds the bandwidth determined by the queue's weighting factor, or the queue is empty. Then the WRR mechanism moves to the next queue. If a queue is empty, the router will send packets from the next queue that has packets ready to send.

Note that if a packet's length exceeds the queue's allowed bandwidth, the packet is still transmitted during its time slot, but its quota is overdrawn so that on the next time slot it receives a smaller allotment. This mechanism guarantees a minimum bandwidth to each queue, but allows the minimum to be exceeded if one or more of the port's other queues are idle. However, when all the queues are loaded each is limited to its maximum bandwidth according to its assigned weight - no queue achieves more than a predetermined proportion of overall capacity when the line is under stress.

The weighting factors are specified as relative percentages, either as the actual number of packets transmitted each turn, or as the byte count transmitted, in 256-byte quanta. The values for all the queues must be positive, and must add up to ten or 100.

If the packet sizes of the queues vary significantly, using byte counts rather than packet values provides a greater degree of bandwidth fairness. For example, suppose one protocol has 500-byte packets, another has 300-byte packets, and a third has 100-byte packets. If you want to split the bandwidth evenly across all three protocols, you might choose to specify byte counts of 200, 200, and 200 for each queue. However, this configuration does not result in a 33/33/33 ratio of bandwidth usage. When the router services the first queue, it sends a single 500-byte packet; when it services the second queue, it sends a 300-byte packet; and when it services the third queue, it sends two 100-byte packets. The effective ratio is 50/30/20 - setting the byte count too low can result in an unintended bandwidth allocation.

However, very large byte counts will produce a "jerky" distribution. That is, if you assign 10 KB, 10 KB, and 10 KB to the three queues in the example given, each protocol is serviced promptly when its queue is the one being serviced, but it may be a long time before the queue

is serviced again. A better solution is to specify 500-byte, 600-byte, and 500-byte counts for the queue. This configuration results in a ratio of 31/38/31, which may be acceptable.

In order to service queues in a timely manner and ensure that the configured bandwidth allocation is as close as possible to the required bandwidth allocation, you should cross-check the byte count resulting from each protocol's packet size, otherwise the results may not match what you wish to configure.

Figure 18-3 shows how WRR queuing behaves.

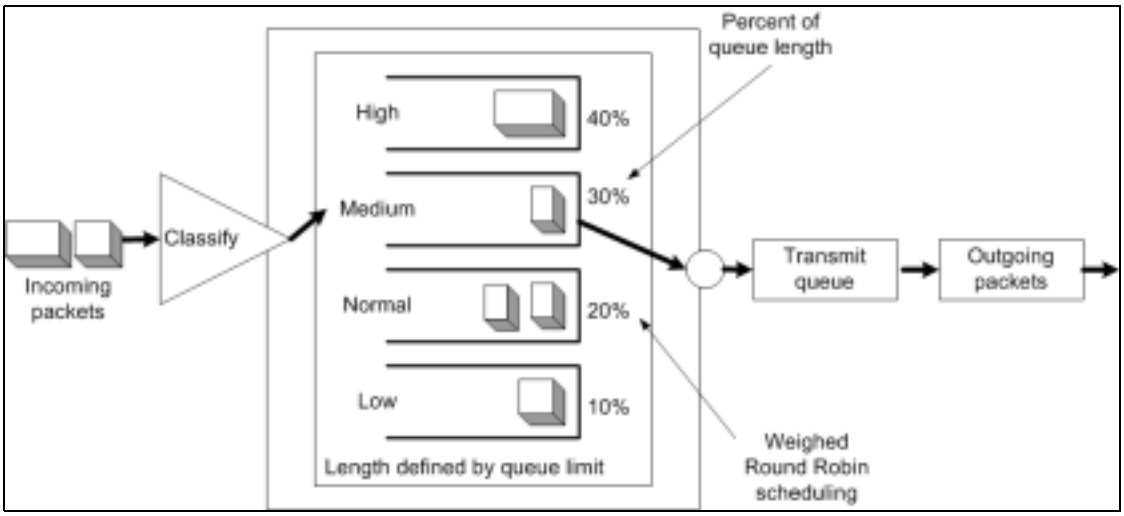


Figure 18-3 Weighted Round Robin Queuing

Benefits of WRR Queuing

WRR scheduling prevents the low-priority queues from being completely neglected during periods of high-priority traffic. By using this scheduling, low-priority queues have the opportunity to transmit packets even though the high-priority queues are not empty.

Byte-Rate Calculations

To check actual byte counts resulting from packet-based allocation:

For each queue, divide the percentage of bandwidth you want to allocate to the queue by the packet size, in bytes. For example, assume the packet size for protocol A is 1086 bytes, protocol B is 291 bytes, and protocol C is 831 bytes. We want to allocate 20 percent for A, 60 percent for B, and 20 percent for C. The ratios would be:

20/1086, 60/291, 20/831 or 0.01842, 0.20619, 0.02407

Normalize the numbers by dividing by the lowest number:

1, 11.2, 1.3

The result is the ratio of the number of packets that must be sent so that the percentage of bandwidth that each protocol uses is approximately 20, 60, and 20 percent.

A fraction in any of the ratio values means that an additional packet will be sent. Round up the numbers to the next whole number to obtain the actual packet count. In this example, the actual ratio will be 1 packet, 12 packets, and 2 packets.

Convert the packet number ratio into byte counts by multiplying each packet count by the corresponding packet size. In this example, the number of packets sent is one 1086-byte packet, twelve 291-byte packets, and two 831-byte packets or 1086, 3492, and 1662 bytes,

respectively, from each queue. These are the byte counts you would specify in your custom queuing configuration.

To determine the bandwidth distribution this ratio represents, first determine the total number of bytes sent after traffic serviced on all of the three queues:

(1 x 1086) + (12 x 291) + (2 x 831) = 1086 + 3492 + 1662 = 6240

Then determine the percentage of the total number of bytes sent from each queue:

1086/6240, 3492/6240, 1662/6240 = 17.4, 56, and 26.6 percent

As you can see, this is close to the desired ratio of 20/60/20.

If the actual bandwidth is not close enough to the desired bandwidth, multiply the original ratio of 1:11.2:1.3 by the best value, trying to get as close to three integer values as possible. Note that the multiplier you use need not be an integer. For example, if we multiply the ratio by two, we get 2:22.4:2.6.We would now send two 1086-byte packets, twenty-three 291-byte packets, and three 831-byte packets, or 2172/6693/2493, for a total of 11,358 bytes. The resulting ration is 19/59/22 percent, which is much closer to the desired ratio that we achieved.

Technique for Avoiding QoS Congestion

The QoS congestion avoidance technique strives to avoid congestion by monitoring network traffic loads at network and internetwork bottlenecks. In conditions of congestion, this technique provides preferential treatment for premium class traffic in order to maximize network throughput and capacity utilization while minimizing packet loss and delay.

Weighted Random Early Detection (WRED) Mechanism

One of the queuing schemes that have lately been gaining prominence is the WRED. Unlike other queuing schemes, it is designed to prevent congestions beforehand, rather than to manage them once they occur. WRED overcomes a situation known as *tail drop*, which occurs when a burst of packets saturates a switch’s or router's buffer causing the last few packets in the burst to be dropped because the buffer has no room left for them.

A *tail drop* is bad because it prevents you from controlling which packets are dropped. Ideally, you would choose to save your high priority packets and allow your low priority packets to be dropped. However, when the buffer is full, packets are lost before you can identify their priorities.

WRED copes with this situation by watching the queues and starting to drop packets when the queues begin to fill up. Dropping a packet or two doesn't save much space, but if a TCP packet is dropped, TCP will throttle down its transmission rate, helping to keep things nice and smooth.

WRED bases its decision about which packet to drop on IP Precedence. It does not check the protocol (i.e. TCP versus UDP). Since most VoIP installations grant higher priority to their VoIP traffic, which is typically UDP, WRED is more likely to drop the lower-priority TCP traffic.

However, if you have a substantial amount of other UDP traffic, you should increase its priority as well, so that your UDP traffic would not be dropped. If your UDP packets are discarded, not only will you lose the packets (which must be retransmitted by the application, if they are retransmitted at all), but also the ability of WRED to prevent the congestion will be

impaired, since UDP does not use the "slow start" flow control mechanism that is used by TCP.

Output Traffic Shaping

When congestion occurs, the packets are transmitted on the outgoing interface and the assigned queues. Traffic shaping allows you to shape output traffic (egress traffic) on a per-port basis and also per queue on the port. The output traffic is monitored to verify that it conforms to the rate configured on the switch. When excessive traffic is detected on the switch, the output interface applies the traffic shaping and controls the excess traffic. If the switch queues overflow, the traffic is dropped.

Supported Standards, MIBs and RFCs

Standards

IEEE 802.1p Priority Queuing

MIBs

No MIBs are supported by this feature.

RFCs

RFC 2697, *A Single Rate Three Color Marker*

RFC 2698, A Two Rate Three Color Marker

Default QoS Configuration

Table 18-1 shows the default QoS configuration.

Table 18-1 Default QoS Configuration

Feature	Default Value
The queue to priority assignment	See table 18-2
The priority to queue assignment	See table 18-3

QoS scheduling algorithm	Strict Priority
Port Priority	0
Port override	No
Port's congestion-avoidance algorithm.	Tail-drop
Drop level per user priority	Green
MAC address priority	0
Traffic shaping	Disabled

Table 18-2 Default Queue to Priority Assignment

Priority	Queue
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

Table 18-3 Default Priority to Queue Assignment

Queue	Priority
7	7
6	6
4	4
3	3
2	2
1	1
0	0

Configuring Quality of Service Features

To set the QoS, proceed as follows:

- To configure mapping of the 802.1p priroity levels to internal transmit queue values, see "Configuring Priority Value Mapping to QoS Queues".
- To configure re-marking of the internal transmit queue values to 802.1p priroity levels, see "Replacing 802.1p Priority Information in Transmitted Packets".
- To override priorty on the incoming traffic per port, see "Replacing 802.1p Priority Information on a Port".
- To set QoS priority manually per destination MAC address, see "Setting the Destination MAC Address Priority".
- To override QoS scheduling algorithm settings, see "QoS Scheduling Commands".
- To set traffic shaping see "Configuring Traffic Shaping".

QoS Priority Mapping Commands

Table 18-4 lists the commands to configure and display the QoS priority mapping commands.

Table 18-4 Priority Mapping Commands

Command	Description
qos map	Assigns 802.1p priority level to the Transmit-Queue mapping.

qos remark	Changes the 802.1p priority of each tagged outgoing packet as it leaves the switch, by assigning an 802.1p priority level to each transmission queue.
show qos priority-txq-map	Displays the priority mapping assignments.

Configuring Priority Value Mapping to QoS Queues

The **qos map** command, in Global Configuration mode, assigns 802.1p priority level to the Transmit-Queue mapping.

Table 18-2 shows the default mapping of priority levels to the eight transmit queues.

Command Syntax

device-name(config)#**qos map** <*priority*> {**txq0**|**txq1**|**txq2**|**txq3**|**txq4**|**txq5**|**txq6**|**txq7**}

Argument Description

priority	**The 802.1p priority level in range <0-7>.**
txq0	Transmit queue 0.
txq1	Transmit queue 1.
txq2	Transmit queue 2.
txq3	Transmit queue 3.
txq4	Transmit queue 4.
txq5	Transmit queue 5.
txq6	Transmit queue 6.
txq7	Transmit queue 7.

Example

The default mapping of 802.1p priority level 3 is txq1. In the following example, we change the mapping of priority level 3 to txq2, and verify the change with the **show qos priority-txq-map** command.

```
device-name(config)#qos map 3 txq2
device-name(config)#exit
device-name#show qos priority-txq-map
==============================
priority-level   | txq
-----------------+-------------
0                | 0
1                | 1
2,3              | 2
                 | 3
4                | 4
5                | 5
6                | 6
7                | 7
```

Replacing 802.1p Priority Information in Transmitted Packets

The **qos remark** command, in Global Configuration mode, changes the 802.1p priority of each tagged outgoing packet as it leaves the switch, by assigning an 802.1p priority level to each transmission queue. All tagged packets leaving the switch through this queue are re-marked with the specified priority.

NOTE The switch does not change the VLAN Priority Tag (VPT) for a switched packet that comes with an 802.1Q tag, since it assumes that the sender of the packet has already determined the VPT.

Packets received without a tag have their VPT set by the command qos remark.

Table 18-3 shows the default re-marking of queues to 802.1p priority levels.

Command Syntax

device-name(config)#**qos remark** *<priority>* {**txq0**|**txq1**|**txq2**|**txq3**|**txq4**|**txq5**|**txq6**|**txq7**}

Argument Description

priority	The 802.1p priority level in range <0-7>.
txq0	Transmit queue 0.
txq1	Transmit queue 1.
txq2	Transmit queue 2.
txq3	Transmit queue 3.
txq4	Transmit queue 4.
txq5	Transmit queue 5.
txq6	Transmit queue 6.
txq7	Transmit queue 7.

Example

In the following example, the **qos remark command** re-marks the 802.1p priority levels for txq1 and tx2 to priority 3 and priority 5 respectively. The **show qos priority-txq-map remark** command prior to the configuration shows the default re-marking levels. Following the configuration, the show command displays the changes.

```
device-name#show qos priority-txq-map remark
================================
priority-level  | txq
----------------+----------------
0               | 0
1               | 1
2               | 2
3               | 3
4               | 4
5               | 5
6               | 6
7               | 7

device-name#configure terminal
```

```
device-name(config)#qos remark 3 txq1
device-name(config)#qos remark 5 txq2
device-name(config)#exit
device-name#show qos priority-txq-map remark
================================
priority-level  | txq
----------------+----------------
0               | 0
3               | 1
5               | 2
3               | 3
4               | 4
5               | 5
6               | 6
7               | 7
```

Displaying the Mapping Assignments

The **show qos priority-txq-map** command, in Privileged (Enable) mode, displays the priority mapping. When the argument **remark** is in use the command will display the reassigned priority level (for re-marking) per each output queue. Otherwise, the command will display the general priority to output queue map.

Command Syntax

```
device-name#show qos priority-txq-map [remark]
```

QoS Assignment Configuration Commands

Table 18-5 lists the commands to configure the priority assignment.

Table 18-5 Priority Assignment Configuration Commands

Command	Description
qos priority	Assigns a priority value that can override the 802.1p priority levels for incoming frames.
qos mac	Assigns QoS priority level manually for destination MAC address (per VLAN).
qos drop-level priority	Specifies the color mark per QoS priority.
qos shaper	Sets the transmit rate for the transmit queue

Replacing 802.1p Priority Information on a Port

The **qos priority** command, in Interface Configuration mode, assigns a priority value that can override the 802.1p priority levels for incoming frames. The **no** form of this command restores the port's priority settings to the default values.

At each port, you can choose to override the 802.1p priority levels by assigning a new value. Consequently, every incoming frame will obtain the new priority level and then be mapped to the appropriate output queue according to the 802.1p level-to-queue mapping.

If you choose not to override the 802.1p priority for incoming frames (by using the **no-override** option), then 802.1p tagged frames will be forwarded according to their own priority

level. Untagged frames (that have no assigned priority) will obtain the priority assigned to them by this command.

By default, all the ports are assigned with priority 0, **no override** option is assigned and the congestion-avoidance algorithm is Tail-drop.

Command Syntax

```
device-name(config-if UU/SS/PP)#qos priority <priority> {override|no-override} {gred|tail}
device-name(config-if UU/SS/PP)#no qos priority
```

Argument Description

priority	The 802.1p priority level in range <0-7>.
override	Override the 802.1p priority level.
no-override	Do not override the 802.1p priority level.
gred	The WRED congestion-avoidance algorithm (GRED stands for General RED – the WRED mechanism with three levels of drop precedence).
tail	The Tail-drop congestion-avoidance algorithm.

Example 1

The following example overrides the 802.1p priority levels for tagged and untagged incoming frames on interface 1/1/1. The show qos priority-txq-map command specifying the interface number verifies the configuration.

```
device-name(config-if 1/1/1)#qos priority 3 override gred
device-name(config-if 1/1/1)#end
device-name#show qos priority 1/1/1
============================================================
Interface | priority-level  | txq  | override | Drop Algorithm
----------+-----------------+------+----------+---------------
 1/ 1/ 1  | 3               | 3    | yes      | GRED
```

Example 2

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#qos priority 3 override tail
device-name(config-if 1/1/1)#exit
device-name(config)#exit
device-name#show qos priority 1/1/1
============================================================
Interface | priority-level  | txq  | override | Drop Algorithm
----------+-----------------+------+----------+---------------
 1/ 1/ 1  | 3               | 3    | yes      | Tail-Drop
```

Setting the Destination MAC Address Priority

The **qos mac** command, in Global Configuration mode, assigns QoS priority level manually per destination MAC address (per VLAN). The **no** form of the command will delete the MAC address.

All traffic destined for a specific MAC address, per VLAN and per port, can be assigned a priority level. The frame is then forwarded to a transmit queue using the mapping of 802.1p to transmit queues.

- To view the priority assignment for the MAC addresses, use the **show mac-address-table** command in Privileged (Enable) mode.
- To clear the MAC addresses with the priority assignment you can also use the **clear mac-address-table** command in Privileged (Enable) mode and the **no mac-address-table** command in Global Configuration mode.

By default, the MAC address priority is 0.

Command Syntax

device-name(config)#**qos mac** {**static**|**secure**} *HH:HH:HH:HH:HH:HH* **vlan** <*vlan-id*> *UU/SS/PP* **priority** <*priority*>
device-name(config)#**no qos mac** [[**static**|*s***ecure**] [*HH:HH:HH:HH:HH:HH*] [**vlan** <*vlan-id*>] [*UU/SS/PP*]]

Argument Description

static	Static MAC address
secure	Secured MAC address, used for Port Security.
HH:HH:HH:HH:HH:HH	6-byte MAC address represented hexadecimally.
vlan <vlan-id>	VLAN ID value (MAC address can be learned on several VLANs) in range of <1-4094>.
UU/SS/PP	Interface's unit/slot/port number.
priority <priority>	Priority given for the MAC address in range of <0-7>.

Example

In the following example, we define two static MAC addresses on the same VLAN and interface. The configured priorities give preference to packets with destination MAC address 00:01:02:03:04:06 over the packets with destination MAC address 00:01:02:03:04:05.

```
device-name(config)#qos mac static 00:01:02:03:04:05 vlan 1 1/1/5
priority 3
device-name(config)#qos mac static 00:01:02:03:04:06 vlan 1 1/1/5
priority 6
device-name(config)#end
device-name#show mac-address-table

===============+==================+=============+==========+=========
  #  |    VID    |  Mac              |  PORT       |  STATUS  |PRIORITY|
-----+-----------+-------------------+-------------+----------+--------+
  1  |   0001    |00:01:02:03:04:05  |  1/1/5      |  static  | 3      |
  2  |   0001    |00:01:02:03:04:06  |  1/1/5      |  static  | 6      |
  3  |   0001    |00:02:b3:1a:bb:87  |  1/1/3      |  dynamic | 0      |
…
 46  |   0001    |00:c1:26:01:1a:6d  |  1/1/3      |  dynamic | 0      |
```

Configuring Drop Level Priority

The **qos drop-level** command, in Global Configuration mode, specifies the color mark per QoS priority. The **no** form of this command resets the priority color marking to the default color.

In a congestion condition within the same queue, color marks define which packets are to be discarded. Color marks express the precedence level for discarding packets.

By default, the drop level is Green.

Command Syntax

```
device-name(config)#qos drop-level priority <priority> {green|yellow|red}
device-name(config)#no qos drop-level priority
```

Argument Description

priority	Priority level value in the range <0-7>.
green	Conforming precedence level.
yellow	Last conforming precedence level.
red	Non conforming precedence level.

Example

The following example configures the drop level priority 1, 2 and 3 and sets the precedence level. The **show qos drop-level** command displays the results.

```
device-name(config)#qos drop-level priority 1 green
device-name(config)#qos drop-level priority 2 red
device-name(config)#qos drop-level priority 3 yellow
device-name(config)#end
device-name#show qos drop-level

======================
 Priority | Drop Level
----------+------------
 0        | green
 1        | green
 2        | red
 3        | yellow
 4        | green
 5        | green
 6        | green
 7        | green
```

Configuring Traffic Shaping

The **qos shaper** command, in Interface Configuration mode, sets the rate for the transmit port or transmit port and queue. Traffic shaping is used to control the rate of outgoing traffic in order to make sure that the traffic conforms to the maximum rate of transmission provided for it. The **no** form of this command removes the traffic shaping.

Each transmit port can be configured to transmit at a specific rate. On each transmit port you can also set the transmit rate for a specific queue. Any traffic that exceeds the configured shaping rate will be queued and transmitted at the configured rate. If the burst of traffic exceeds the size of the queue, packets will be dropped to maintain transmission at the configured shaping rate.

By default, no traffic shaping is assigned.

NOTE  Since the rate granularity is limited, whenever you set the rate you will see a message specifying the rate that is actually configured.

Command Syntax

```
device-name(config-if UU/PP/SS)#qos shaper [queue <value>] rate <rate-size> burst <burst-size>
```

```
device-name(config-if UU/PP/SS)#no qos shaper [queue <value>]
```

Argument Description

queue <value>	(Optional). The transmit queue with value in range of <0-7>.
rate <rate-size>	The shaping rate in bps, represented by an integer followed by k, m or g (Kilobits, Megabits or Gigabits per second) in the range <650Kbps – 1Gbps>). Granularity is 650Kbps. Values not matching this granularity will be rounded.
burst <burst-size>	The burst size in units of 4 Kilobits. The range is <1-4095>.

Example

The following example configures the transmit rate of 2M to the transmit queue 2. The **show qos shaper** command displays the results:

```
device-name(config-if 1/1/1)#qos shaper queue 2 rate 2m burst 16
device-name(config-if 1/1/1)#end
device-name#show qos shaper

Interface 1/1/1
==================
qos shaper queue 2 rate 2M burst 64K
```

QoS Assignment Displaying Commands

Table 18-6 lists the commands to display the priority assignment.

Table 18-6 Available Priority Assignment Displaying Commands

Command	Description
show qos priority-txq-map	Displays the port priority mapping.
show qos drop-level	Displays the Drop level priority mapping.
show qos shaper	Displays the transmit rate for the transmit queue.

Displaying the Mapping Assignments

The **show qos priority-txq-map** command, in Privileged (Enable) mode, displays the port priority mapping.

Command Syntax

```
device-name#show qos priority-txq-map {UU/SS/PP | all}
```

Argument Description

UU/SS/PP	The unit, slot and port of a specific interface.
all	Displays the QoS configuration of the entire interface.

Example

```
device-name#show qos priority all
```

```
=============================================================
Interface | priority-level  | txq  | override | Drop Algorit
----------+-----------------+------+----------+-------------
 1/ 1/ 1  | 3               | 3    | yes      | GRED
 1/ 1/ 2  | 0               | 0    | no       | Tail-Drop
 1/ 1/ 3  | 0               | 0    | no       | Tail-Drop
…
 1/ 1/48  | 0               | 0    | no       | Tail-Drop
 1/ 2/ 1  | 0               | 0    | no       | Tail-Drop
 1/ 2/ 2  | 0               | 0    | no       | Tail-Drop
 1/ 2/ 3  | 0               | 0    | no       | Tail-Drop
```

Displaying Drop Level Priority

The **show qos drop-level** command, in Privileged (Enable) mode, displays the Drop level priority mapping.

Command Syntax

```
device-name#show qos drop-level
```

Example

```
device-name#show qos drop-level

=======================
 Priority | Drop Level
----------+------------
 0        | green
 1        | green
 2        | red
 3        | yellow
 4        | green
 5        | green
 6        | green
 7        | green
```

Displaying Traffic Shaping

The **show qos shaper** command, in Privileged (Enable) mode, displays the transmit rate for the transmit port or transmit port and queue.

NOTE Since the rate granularity is limited, whenever you set the rate you will see a message specifying the rate that is actually configured.

Command Syntax

```
device-name#show qos shaper
```

Example

```
device-name#show qos shaper

Interface 1/1/1
==================
qos shaper queue 2 rate 2M burst 64K
 1/ 2/ 4  | 0               | 0    | no       | Tail-Drop
```

QoS Scheduling Commands

A QoS scheduling command overrides any previous QoS scheduling command applied to the configured interface, globally or specifically. This means that:

If you configure QoS in Global Configuration mode, and subsequently configure a specific port in Interface Configuration mode, the last configuration is applied to the specific interface.

If you apply QoS commands in a specific port's Interface Configuration mode, and subsequently reconfigure QoS in global Configuration mode, the last command takes effect for all interfaces, including the specific interface.

Table 18-7 lists the commands to configure and display the QoS scheduling algorithms.

Table 18-7 Available QoS Scheduling Commands

Command	Description
qos scheduling sp	Configures Strict Priority (SP) scheduling.
qos scheduling wrr	Configures Weighted Round-Robin (WRR) scheduling.
qos scheduling hybrid-1	Configures first hybrid-type scheduling.
qos scheduling hybrid-2	Configures second hybrid-type scheduling.
qos scheduling hybrid-3	Configures from 3rd hybrid-type scheduling.
qos scheduling hybrid-4	Configures from 4th hybrid-type scheduling.
qos scheduling hybrid-5	Configures from 5th hybrid-type scheduling.
qos scheduling hybrid-6	Configures from 6th hybrid-type scheduling.
show qos scheduling	Displays the current QoS scheduling settings.

Configuring Strict Priority QoS Queue Handling

The **qos scheduling sp** command, in Global Configuration or Interface Configuration mode, configures SP (Strict Priority) scheduling.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling sp
```

Configuring Weighted Round-Robin QoS Queue Handling

The **qos scheduling wrr** command, in Global Configuration or Interface Configuration mode, applies and configures Weighted Round-Robin (WRR) scheduling. In WRR scheduling, bandwidth is allocated proportionally for each queue. Network resources are shared among all of the applications you service, each having the specific bandwidth requirements you have identified.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling wrr  <txq0-weight> <txq1-weight> <txq2-
weight> <txq3-weight> <txq4-weight> <txq5-weight> <txq6-weight> <txq7-weight>
```

Argument Description

<txq0-weight> ... <txq7-weight>	The weights assigned to the transmit queues. The eight values must be positive and add up to 10 or 100.

Example

The following example assigns weights 1, 1, 1, 1, 2, 2, 1, 1 to transmit queues txq0 to txq7 respectively on all ports. It then assigns weights 1, 1, 1, 1, 1, 1, 2, 2 to the transmit queues on port 1/1/1, and weights 1, 1, 1, 1, 1, 2, 2, 1 to the transmit queues on port 1/1/2. The **show qos scheduling** command displays the results on all ports.

```
device-name(config)#qos scheduling wrr 1 1 1 1 2 2 1 1
device-name(config)#int 1/1/1
device-name(config-if 1/1/1)#qos scheduling wrr 1 1 1 1 1 1 2 2
device-name(config-if 1/1/1)#int 1/1/2
device-name(config-if 1/1/2)#qos scheduling wrr 1 1 1 1 1 2 2 1
device-name(config-if 1/1/2)#exit
device-name config)#exit
device-name#show qos scheduling all
================================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 1  | wrr        |  1 |  1 |  1 |  1 |  1 |  1 |  2 |  2 |
 1/ 1/ 2  | wrr        |  1 |  1 |  1 |  1 |  1 |  2 |  2 |  1 |
 1/ 1/ 3  | wrr        |  1 |  1 |  1 |  1 |  2 |  2 |  1 |  1 |
 . . .
 1/ 1/48  | wrr        |  1 |  1 |  1 |  1 |  2 |  2 |  1 |  1 |
 1/ 2/ 1  | wrr        |  1 |  1 |  1 |  1 |  2 |  2 |  1 |  1 |
 1/ 2/ 2  | wrr        |  1 |  1 |  1 |  1 |  2 |  2 |  1 |  1 |
 1/ 2/ 3  | wrr        |  1 |  1 |  1 |  1 |  2 |  2 |  1 |  1 |
 1/ 2/ 4  | wrr        |  1 |  1 |  1 |  1 |  2 |  2 |  1 |  1 |
```

Configuring Hybrid-1 QoS Queue Handling

The **qos scheduling hybrid-1** command, in Global Configuration or Interface Configuration mode, applies and configures the first hybrid QoS algorithm.

In the first hybrid algorithm, *txq7* is assigned strict priority scheduling, and the remaining queues are assigned Weighted Round Robin (WRR) scheduling. According to this configuration:

txq7 is serviced as long as it has packets for transmission.

When *txq7* is empty, the remaining queues are serviced according to their assigned weights.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling hybrid-1 <txq0-weight> <txq1-weight>
<txq2-weight> <txq3-weight> <txq4-weight> <txq5-weight> <txq6-weight>
```

Argument Description

<txq0-weight> ... <txq6-weight>	The weights assigned to the weighted transmit queues. The values must be positive and add up to 10 or 100.

Example

The following example configures hybrid-1 scheduling on port 1/1/3. The **show qos scheduling** command displays the results on the specified port.

```
device-name(config)#int 1/1/3
device-name(config-if 1/1/3)#qos scheduling hybrid-1  1 1 2 2 2 1 1
device-name(config-if 1/1/3)#end
device-name#show qos scheduling 1/1/3
=============================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 3  | hybrid-1   |  1 |  1 |  2 |  2 |  2 |  1 |  1 |
```

Configuring Hybrid-2 QoS Queue Handling

The **qos scheduling hybrid-2** command, in Global Configuration or Interface Configuration mode, is used to apply and configure the second hybrid QoS algorithm.

In the second hybrid algorithm, *txq6* and *txq7* are set to behave according to strict priority scheduling, and the rest of the queues behave according to Weighted Round Robin (WRR). According to this configuration:

- *tqx7* is serviced as long as it has packets for transmission.
- When *txq7* is empty, *txq6* is serviced as long as it has packets.
- When both *txq6* and *txq7* are empty, the rest of the queues are serviced according to their assigned weights.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling hybrid-2 <txq0-weight> <txq1-
weight> <txq2-weight> <txq3-weight> <txq4-weight> <txq5-weight>
```

Argument Description

<txq0-weight> ... <txq5-weight>	The weights assigned to the weighted transmit queues. The values must be positive and add up to 10 or 100.

Example

The following example configures hybrid-2 scheduling on port 1/1/4. The **show qos scheduling** command displays the results on the specified port.

```
device-name(config-if 1/1/4)#qos scheduling hybrid-2 packets 10 10 10 20 20 30
device-name(config-if 1/1/4)#end
device-name#show qos scheduling 1/1/4
=============================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 4  | hybrid-2   | 10 | 10 | 10 | 20 | 20 | 30 |    |
```

Configuring Hybrid-3 QoS Queue Handling

The **qos scheduling hybrid-3** command, in Global Configuration or Interface Configuration mode, is used to apply and configure the third hybrid QoS algorithm.

In the third hybrid algorithm, *txq5*, *txq6* and *txq7* are set to behave according to strict priority scheduling, and the rest of the queues behave according to Weighted Round Robin (WRR). According to this configuration:

- *tqx7* is serviced as long as it has packets for transmission.
- When *txq7* is empty, *txq6* is serviced as long as it has packets.
- When *txq6* is empty, *txq5* is serviced as long as it has packets.
- When *txq5*, *txq6* and *txq7* are empty, the rest of the queues are serviced according to their assigned weights.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling hybrid-3 <txq0-weight> <txq1-
weight> <txq2-weight> <txq3-weight> <txq4-weight>
```

Argument Description

<txq0-weight> ... <txq4-weight>	The weights assigned to the weighted transmit queues. The values must be positive and add up to 10 or 100.

Example

The following example configures hybrid-3 scheduling on port 1/1/4. The **show qos scheduling** command displays the results on the specified port.

```
device-name(config-if 1/1/4)#qos scheduling hybrid-3 packets 10 10 20 20 40
device-name(config-if 1/1/4)#end
device-name#show qos scheduling 1/1/4
================================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 4  | hybrid-3   | 10 | 10 | 20 | 20 | 40 |    |    |
```

Configuring Hybrid-4 QoS Queue Handling

The **qos scheduling hybrid-4** command, in Global Configuration or Interface Configuration mode, is used to apply and configure the forth hybrid QoS algorithm.

In the forth hybrid algorithm, *txq4*, *txq5*, *txq6* and *txq7* are set to behave according to strict priority scheduling, and the rest of the queues behave according to Weighted Round Robin (WRR). According to this configuration:

- *tqx7* is serviced as long as it has packets for transmission.
- When *txq7* is empty, *txq6* is serviced as long as it has packets.
- When *txq6* is empty, *txq5* is serviced as long as it has packets.
- When *txq5* is empty, *txq4* is serviced as long as it has packets.
- When *txq4*, *txq5*, *txq6* and *txq7* are empty, the rest of the queues are serviced according to their assigned weights.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling hybrid-4 <txq0-weight> <txq1-
weight> <txq2-weight> <txq3-weight>
```

Argument Description

<txq0-weight> ... <txq3-weight>	The weights assigned to the weighted transmit queues. The values must be positive and add up to 10 or 100.

Example

The following example configures hybrid-4 scheduling on port 1/1/4. The **show qos scheduling** command displays the results on the specified port.

```
device-name(config-if 1/1/4)#qos scheduling hybrid-4 packets 10 20 30 40
device-name(config-if 1/1/4)#end
device-name#show qos scheduling 1/1/4
============================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 4  | hybrid-4   | 10 | 20 | 30 | 40 |    |    |    |
```

Configuring Hybrid-5 QoS Queue Handling

The **qos scheduling hybrid-5** command, in Global Configuration or Interface Configuration mode, is used to apply and configure the fifth hybrid QoS algorithm.

In the fifth hybrid algorithm, *txq3*, *txq4*, *txq5*, *txq6* and *txq7* are set to behave according to strict priority scheduling, and the rest of the queues behave according to Weighted Round Robin (WRR). According to this configuration:

- *tqx7* is serviced as long as it has packets for transmission.
- When *txq7* is empty, *txq6* is serviced as long as it has packets.
- When *txq6* is empty, *txq5* is serviced as long as it has packets.
- When *txq5* is empty, *txq4* is serviced as long as it has packets.
- When *txq4* is empty, *txq3* is serviced as long as it has packets.
- When *txq3*, *txq4*, *txq5*, *txq6* and *txq7* are empty, the rest of the queues are serviced according to their assigned weights.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling hybrid-4 <txq0-weight> <txq1-weight> <txq2-weight>
```

Argument Description

<txq0-weight> ... <txq2-weight>	The weights assigned to the weighted transmit queues. The values must be positive and add up to 10 or 100.

Example

The following example configures hybrid-5 scheduling on port 1/1/4. The **show qos scheduling** command displays the results on the specified port.

```
device-name(config-if 1/1/4)#qos scheduling hybrid-5 packets 20 30 50
device-name(config-if 1/1/4)#end
device-name#show qos scheduling 1/1/4
============================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 4  | hybrid-5   | 20 | 30 | 50 |    |    |    |    |
```

Configuring Hybrid-6 QoS Queue Handling

The **qos scheduling hybrid-6** command, in Global Configuration or Interface Configuration mode, is used to apply and configure the sixth hybrid QoS algorithm.

In the sixth hybrid algorithm, *txq2*, *txq3*, *txq4*, *txq5*, *txq6* and *txq7* are set to behave according to strict priority scheduling, and the rest of the queues behave according to Weighted Round Robin (WRR). According to this configuration:

- *tqx7* is serviced as long as it has packets for transmission.
- When *txq7* is empty, *txq6* is serviced as long as it has packets.
- When *txq6* is empty, *txq5* is serviced as long as it has packets.
- When *txq5* is empty, *txq4* is serviced as long as it has packets.
- When *txq4* is empty, *txq3* is serviced as long as it has packets.
- When *txq4* is empty, *txq2* is serviced as long as it has packets.
- When *txq2*, *txq3*, *txq4*, *txq5*, *txq6* and *txq7* are empty, the rest of the queues are serviced according to their assigned weights.

By default, the SP scheduling is applied.

Command Syntax

```
device-name(config)#qos scheduling hybrid-4 <txq0-weight> <txq1-weight> <txq1-weight>
```

Argument Description

<txq0-weight> ... <txq1-weight>	The weights assigned to the weighted transmit queues. The values must be positive and add up to 10 or 100.

Example

The following example configures hybrid-6 scheduling on port 1/1/4. The **show qos scheduling** command displays the results on the specified port.

```
device-name(config-if 1/1/4)#qos scheduling hybrid-6 packets 40 60
device-name(config-if 1/1/4)#end
device-name#show qos scheduling 1/1/4
============================================================
Interface | scheduling |txq0|txq1|txq2|txq3|txq4|txq5|txq6|txq7
----------+------------+----+----+----+----+----+----+----+----
 1/ 1/ 4  | hybrid-6   | 40 | 60 |    |    |    |    |    |
```

Displaying QoS Scheduling Settings

The **show qos scheduling** command, in Privileged (Enable) mode, displays the current QoS scheduling settings.

Command Syntax

```
device-name#show qos scheduling {UU/SS/PP | all}
```

Argument Description

UU/SS/PP	Display the scheduling settings for the specified interface.
all	Display the scheduling settings for all the interfaces.

Related Commands

Table 18-8 shows commands related to QoS configuration.

Table 18-8 QoS Related Commands

Command	Description	Described in
`clear mac-address-table`	Clears the specified MAC addresses.	Understanding and Configuring MAC Address Table
`no mac-address-table`	Clears the specified MAC addresses.	Understanding and Configuring MAC Address Table
`show mac-address-table`	Displays the specified data pertaining to the MAC address table.	Understanding and Configuring MAC Address Table

19. DHCP Client

DHCP Overview

DHCP (Dynamic Host Configuration Protocol) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP, based on the Bootstrap Protocol (BOOTP), adds the capability of automatic allocation of reusable network addresses and additional configuration options. DHCP captures the behavior of BOOTP relay agents and DHCP participants can interoperate with BOOTP participants.

DHCP is described in RFC 2131: *Dynamic Host Configuration Protocol* and in RFC 2132: *DHCP Options and BOOTP Vendor Extensions*.

DHCP provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocating network addresses to hosts.

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. Throughout the remainder of this chapter, the term **server** refers to a host providing initialization parameters through DHCP, and the term **client** refers to a host requesting initialization parameters from a DHCP server.

DHCP supports three mechanisms for IP address allocation:

- *Automatic allocation* - DHCP assigns a permanent IP address to a client.
- *Dynamic allocation* - DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address). Dynamic allocation allows automatic reuse of an address that is no longer needed by the client to which it was assigned. Thus, dynamic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Dynamic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are scarce and it is important to reclaim them when old clients are retired
- *Manual allocation* - a client's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the client. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator. Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses in environments where (for whatever reasons) it is desirable to manage IP address assignments outside of the DHCP mechanisms.

The Nokia ESB26 switch uses two bytes in the client-identifier field of the DHCP message to identify the location of the chassis and the slot that contains the switch. The location is specified by a twelve-bit number and the slot number is specified by a four-bit number. The two remaining bytes in the client-identifier field have a fixed value of zero. You can view the chassis location and slot ID by using the **show positioning** command described in Displaying the Slot and Location.

The ESB26 Startup Process

When the Nokia ESB26 switch resets or is powered on, it first checks whether it has a valid startup configuration file. If the configuration file exists and verifies OK, the further startup process depends on whether or not DHCP is enabled on the switch.

If DHCP has been specifically disabled (i.e. a valid configuration file with "DCHP=disabled" setting has been found in the non-volatile memory), the switch configures using the startup configuration file and starts its normal operation. If, which is the most common case, DHCP is enabled, the switch activates the DHCP Client to update the configuration. If a new configuration is available, it is downloaded replacing the old one and the switch reconfigures from the new file. Detailed description of the DHCP clent behavior during this process follows as a separate section below.

If, at the power-on checkup, the existing configuration file proves to be corrupt, the switch closes all LAN-ports, turning thus inoperable (so called "Closed mode"). (By default, the startup configuration consistency check is performed when it is being read from the non-volatile memory.) In this state, the startup process halts and, of course, no further configuration steps (like sending DHCP requests and configuration updates) will be taken.

If, at the power-on checkup, it turns out that there is no configuration file at all, as in case of a brand-new card, the device uses the factory default settings, namely, all LAN ports enabled with auto negotiation on, no VLANs, Rapid STP and DHCP enabled. In this scenario, because being enabled, the DHCP client will next attempt to obtain an IP address and configure the switch. For the factory-preset IP address and the related settings, refer to the Ex-Factory Default Settings table in the Specifications chapter.

The entrire startup process is schematically presented in Figure 19-1.

DHCP Client Behavior at Startup

As evident from the earlier paragraphs, the DHCP Client is executed at startup in two cases:

1. As part of the normal boot process, if DHCP is enabled;
2. In case of a missing configuration file (when the switch reverts to its ex-factory defaults).

In these cases, the switch activates the DHCP Client and requests the configuration file name from the DHCP Server together with an IP address, subnet mask, and default gateway. When the the file name is received, the DHCP client compares this file name to the name of the existing configuration file. If the names match, it is assumed that the existing configuration file is up to date, so it is used to configure the switch.

If the filenames do not match, the existing configuration file is assumed obsolete and due to be replaced by the one on the server. The TFTP Client then activates to download the file. (This configuration file always resides on a TFTP server.) Once the new configuration file is downloaded, its consistency is checked and if it verifies OK, it is saved to the non-volatile memory and the swicth configures using the new configuration. If the newly downloaded file proves corrupt, it is discarded and the existing configuration file is used instead (or the swich goes into Closed mode, respectively, if there has been no configuration file).

The No IP Error Scenario

The above behavior of the DHCP client assumes that it has successfully received an IP address from the DHCP server. If, however, the IP address has not been received, the DHCP client will keep re-sending the request at predefined time intervals until it eventually manages to negotiate an IP address. (For the exact behavior of the DHCP client and managing its retransmission timeout, refer to Changing the DHCPDISCOVER Messages Retransmission Timeout chapter.)

NOTES

1. The DHCP client is toggled on/off with the **(no) ip address dhcp** command.
2. You can choose whether to save the downloaded configuration to the non-volatile memory. This is managed with the **dhcp-client save-config** command.

For details on these commands, refer to Configuring the DHCP Client chapter.

The entrire startup process is schematically presented in Figure 19-2. It uses asterisks (*), to indicate the following:

*	This configuration is saved to the non-volatile memory;
**	File consistency is tested by a check-sum algorithm;
****	This means that there is no startup configuration file.

The DHCP Negotiation Process

As shown in Table 19-1, the parameter negotiation starts with a DHCPDISCOVER broadcast message from the client seeking a DHCP server. The DHCP Server responds with a DHCPOFFER unicast message offering configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client. The client returns a DHCPREQUEST broadcast message requesting the offered IP address from the DHCP Server. The DHCP Server responds with a DHCPACK unicast message confirming that the IP address has been allocated to the client.

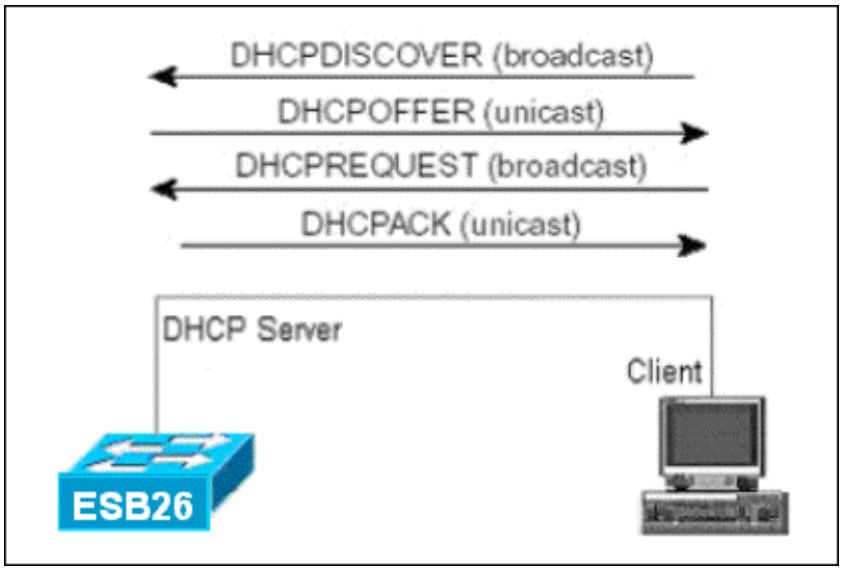


Figure 19-1 Obtaining an IP Address from a DHCP Server

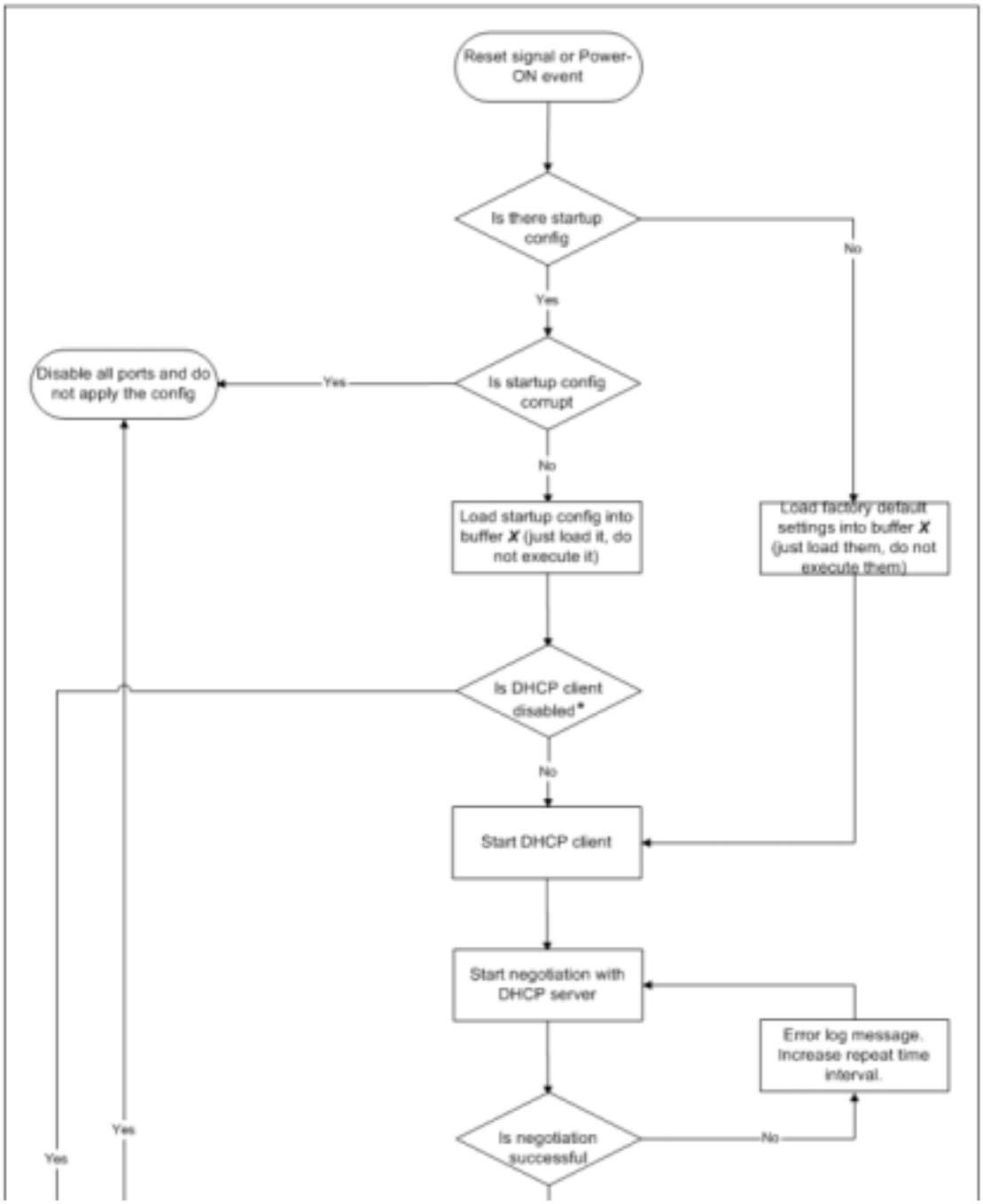
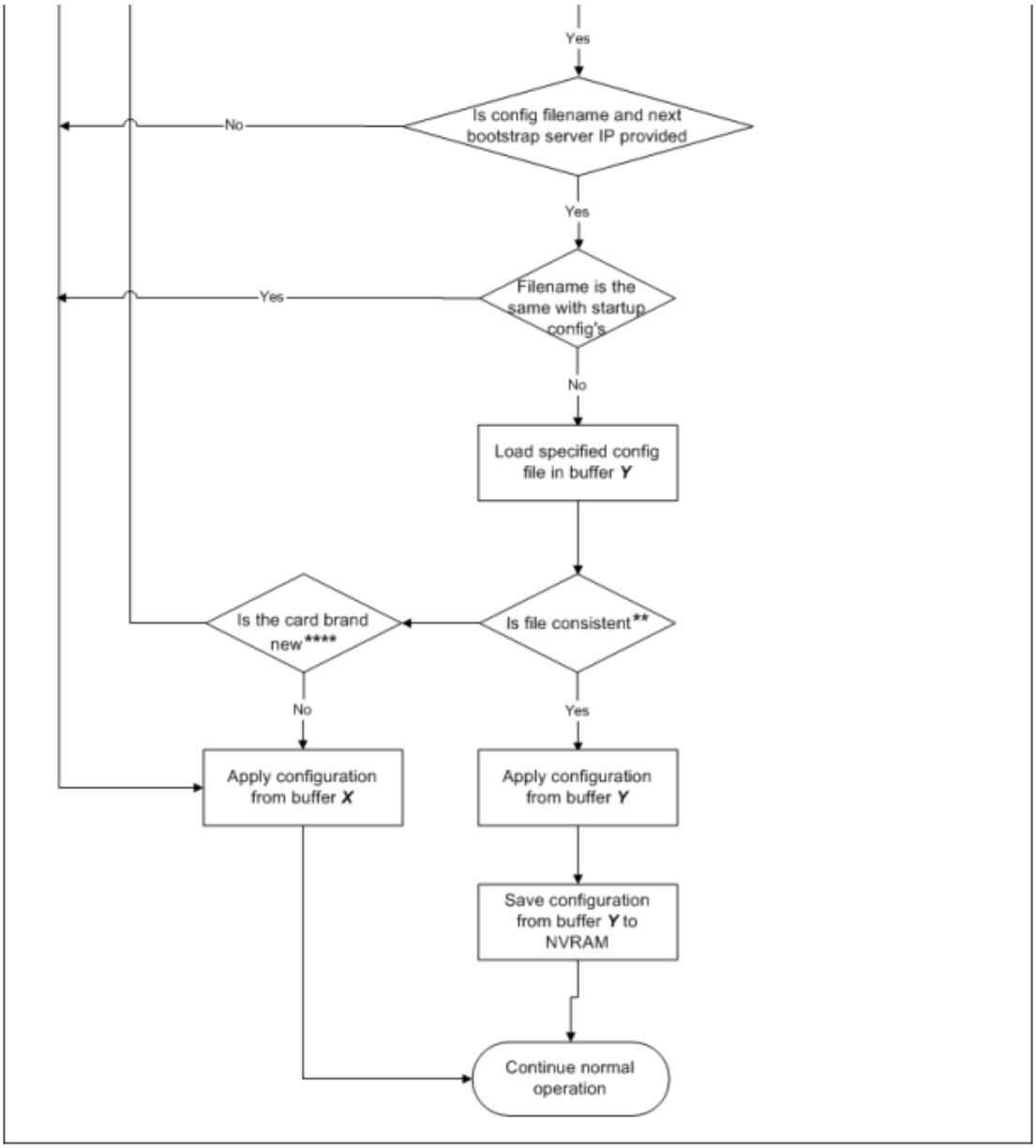


Figure 19-2 Schematic Representation of the Boot Process
(continued on the next page)



The client may suggest values for the IP address and lease time in the DHCPDISCOVER message. The client may include the *requested IP address* option to suggest that a particular IP address be assigned, and may include the *IP address lease time* option to suggest the lease time it would like to have. The *requested IP address* option is to be filled in only in a DHCPREQUEST message when the client is verifying network parameters obtained previously.

If a server receives a DHCPREQUEST message with an invalid *requested IP address*, the server should respond to the client with a DHCPNAK message and may choose to report the problem to the system administrator. The server may include an error message in the *message* option.

When to Use DHCP?

A client should use DHCP to reacquire or verify its IP address and network parameters whenever the local network parameters may have changed (e.g. at the switch boot time or after a disconnection from the local network), as the local network configuration may change without the client's or user's knowledge.

If a client has knowledge of a previous network address and is unable to contact a local DHCP server, the client may continue to use the previous network address until the lease for that address expires. If the lease expires before the client can contact a DHCP server, the client must immediately discontinue use of the previous network address and may inform local users of the problem.

Benefits

By using the DHCP, the time required by a client to configure and deploy the IP address is reduced. The configuration error can also be reduced and the costumers can control the assigned IP address.

Configuring the DHCP Client

Table 19-1 lists the DHCP client commands.

Table 19-1 DHCP Client Commands

Command	Description
ip address dhcp	Provides the switch its IP configuration information dynamically.
dhcp-client discover-rto	Sets the DHCPDISCOVER message retransmission timeout.
show dhcp-client	Displays the DHCP client configuration.
show positioning	Displays the slot and location of the Nokia ESB26 switch.
dhcp-client save-config	Saves the configuration file that is loaded from a TFTP server.

Enabling the DHCP Client

The **ip address dhcp** command, in Global Configuration mode, provides the switch with its IP configuration information dynamically. The DHCP client starts and begins DHCP negotiation. If the IP address is specified, the DHCP client sends a request for this address, and if the requested IP address is not available, the server returns another IP address. The **no**

form of this command stops the DHCP client and restores the IP address, subnet mask and IP gateway to their default values (using the command **ip address**).

By default, the dynamic address allocation is enabled.

To see the allocated IP address, use the **show ip** command in Privileged (Enable) mode.

Command Syntax

```
device-name(config)#ip address dhcp [A.B.C.D]
device-name(config)#no ip address dhcp
```

Argument Description

A.B.C.D	The requested IP address.

Changing the DHCPDISCOVER Messages Retransmission Timeout

The **dhcp-client discover-rto** command, in Global Configuration mode, defines the maximum time that the DHCP client is allowed to be active and to send DHCPDISCOVER frames. By default, the DHCPDISCOVER timeout is disabled.

When the DHCP client lauches, it attempts to negotiate an IP address from the DHCP server. If, however, the IP address has not been received after the first attempt, the DHCP client will keep re-sending the request at predefined time intervals until it eventually manages to negotiate an IP address. The second request will be send one second after the initial one and for each subsequent request, the time interval will increase exponentially by the factor of two (2, 4, 8, 16, 32, 64) until the limiting value of 64 seconds is reached. From this point onward, the DHCP client proceeds by sending its requests at 64-second intervals.

The **no** form of this command disables the retransmission timeout, i.e. the DHCP client will keep sending requests until it negotiates an IP address.

Command Syntax

```
device-name(config)#dhcp-client discover-rto <time>
device-name(config)#no dhcp-client discover-rto
```

Argument Description

time	The DHCPDISCOVER message retransmission timeout in range of <1-32> minutes.

Saving the Configuration File (Boot File)

The **dhcp-client save-config** command, in Global Configuration mode, enables or disables the saving of the configuration file that is loaded by the TFTP client.

By default, this feature is disabled.

Command Syntax

```
device-name(config)#dhcp-client save-config [on|off]
```

Displaying the DHCP Client Configuration

The **show dhcp-client** command, in Privileged (Enable) mode, displays the DHCP client status and the DISCOVER message timeout.

Command Syntax

```
device-name#show dhcp-client
```

Example

```
device-name(config)#ip address dhcp
device-name(config)#exit
device-name#show dhcp-client
DHCP client is active
IP address is acquired by DHCP
DISCOVER messages retransmission timeout is infinite
Lease time left: 61
```

Displaying the Slot and Location

The **show positioning** command, in Privileged (Enable) mode, displays the chassis and slot numbers of the switch.

NOTE The chassis number is displayed in hexadecimal format.

Command Syntax

```
device-name#show positioning
```

Example

```
device-name#show positioning
Current system Slot 04 Location 2ea6s
```

Configuration Example

Figure 19-3 shows a simple network diagram of a DHCP client on an Ethernet LAN.

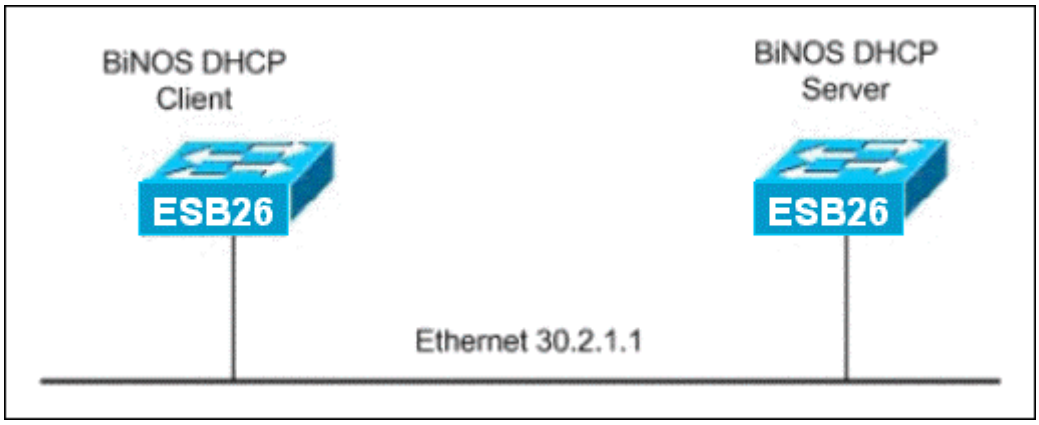


Figure 19-3 Topology Showing DHCP Client with Ethernet Interface

1. The following command enables DHCP client configuration:

```
device-name(config)#ip address dhcp
```

2. The following command displays the DHCP Client Configuration:

```
device-name(config)#exit
device-name#show dhcp-client
DHCP client is active
IP address is acquired by DHCP
DISCOVER messages retransmission timeout - 1 minute(s)
Lease time left: 35
```

20. IGMP Snooping

Introduction

The BiNOS switch can use IGMP (Internet Group Management Protocol) snooping to constrain the flooding of multicast traffic. This is done by dynamically configuring physical interfaces to forward multicast traffic only to interfaces that are associated with IP multicast devices. IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports.

When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry. When it receives an *IGMP Leave Group* message from a host, it removes the host port from the table entry. It also deletes entries periodically if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send *join* requests and are added to the forwarding table entry. The switch forwards only one *join* request per IP multicast group to the multicast router. It creates one entry per VLAN in the forwarding table for each MAC group from which it receives an IGMP *join* request.

Multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping vlan static** configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group, it sends an unsolicited *IGMP join* message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. Hosts wanting to join the multicast group respond by sending a *join* message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the *join* message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group.

Leaving a Multicast Group

The router sends periodic multicast general queries and the switch forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wishes to receive multicast traffic, the router continues forwarding the multicast

traffic to the VLAN. The switch forwards multicast group traffic only to those hosts listed in the forwarding table for that multicast group.

When hosts want to leave a multicast group, they can leave silently or send a *leave* message. When the switch receives a *leave* message from a host, it sends out a MAC-based general query to determine if any other devices connected to that interface are interested in traffic for the specific multicast group. The switch then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

Immediate-Leave Processing

IGMP snooping **Immediate-Leave** processing allows the switch to remove an interface that sends a *leave* message from the forwarding table, without first sending out MAC-based general queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original *leave* message. Immediate-Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

IGMP Snooping Commands

The following IGMP Snooping commands are available.

Table 20-1 IGMP Snooping Commands

Command	Description
ip igmp snooping	Enables IGMP snooping in all existing VLAN interfaces.
ip igmp snooping vlan	Enables the VLAN id for the multicast group.
ip igmp snooping vlan mrouter	Adds a multicast router port (adds a static connection to a multicast router).
ip igmp snooping vlan static	Configures a Host or physical interface statically to join a multicast group.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave Processing on the VLAN interface.
ip igmp snooping for-all	Forwards all multicast via the port list.
ip igmp snooping forbidden	Forbids IGMP snooping via the port list.
ip igmp snooping send-query	Queries sending.
show ip igmp snooping	Displays snooping configuration information for the switch or for a specified VLAN.
show ip igmp snooping mrouter	Displays information on dynamically learned and manually configured multicast router interfaces.

show ip igmp snooping router-timers	Displays the multicast router timer (RFC 2236) to synchronize IGMP snooping.
show ip igmp snooping send-query	Displays Query sending parameters.
show mac-address-table multicast igmp	Displays MAC address table entries for a VLAN.
show ip igmp snooping statistics	Displays Statistics from IGMP snooping.
clear ip igmp snooping	Clears IGMP snooping statistics.

Commands to Configure IGMP Snooping

ip igmp snooping

The **ip igmp snooping** command, in Global Configuration mode, enables IGMP snooping on all existing VLAN interfaces. The **no** form of this command disables IGMP snooping on all existing VLAN interfaces.

By default, IGMP snooping is globally disabled on the switch. When enabled or disabled globally, it is also enabled or disabled in all existing VLAN interfaces. IGMP snooping is by default enabled on all VLANs, but can be enabled or disabled on a per-VLAN basis. After you configure a VLAN interface for multicast routing, no configuration is needed for the switch to access external multicast routers dynamically by using IGMP snooping.

When you enable IGMP snooping, the switch automatically learns the interfaces to which multicast routers are connected. When you disable IGMP snooping, the entire configuration is erased.

Global IGMP snooping overrides VLAN IGMP snooping. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable VLAN snooping.

Command Syntax

```
device-name(config)#ip igmp snooping
device-name(config)#no ip igmp snooping
```

ip igmp snooping vlan

The **ip igmp snooping vlan** command, in Global Configuration mode, enables IGMP snooping on the specified VLAN. By default, IGMP snooping is enabled on all the VLANs. To remove IGMP snooping from a VLAN, use the **no** form of this command.

Command Syntax

```
device-name(config)#ip igmp snooping vlan <vlan-id>
device-name(config)#no ip igmp snooping vlan <vlan-id>
```

Argument Description

vlan-id	the VLAN ID in the range <1-4094>

Example

```
device-name(config)#ip igmp snooping vlan 200
```

ip igmp snooping vlan mrouter

The **ip igmp snooping vlan mrouter** command, in Global Configuration mode, adds a multicast router port (adds a static connection to a multicast router) to a specific VLAN. To remove the multicast router port definition on the specific VLAN, use the **no** form of this command.

Command Syntax

```
device-name(config)#ip igmp snooping vlan <vlan-id> mrouter interface
<UU/SS/PP>
device-name(config)#no ip igmp snooping vlan <vlan-id> mrouter interface
<UU/SS/PP>
```

Argument Description

vlan-id	the multicast router VLAN ID in the range <1-4094>
UU/SS/PP	The interface to the multicast router.

Example

```
device-name(config)#ip igmp snooping vlan 200 mrouter interface 1/1/1
```

ip igmp snooping vlan static

The **ip igmp snooping vlan static** command, in Global Configuration mode, configures a Host or physical interface statically to join a multicast group. The **no** form of this command removes the static multicast definition.

Hosts or physical interfaces normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Command Syntax

```
device-name(config)#ip igmp snooping vlan <vlan-id> static HH:HH:HH:HH:HH:HH
interface PORT-LIST
device-name(config)#no ip igmp snooping vlan <vlan-id> static
HH:HH:HH:HH:HH:HH interface PORT-LIST
```

Argument Description

vlan-id	<1-4094> VLAN id value
HH:HH:HH:HH:HH:HH	6-byte hexadecimal address, should begin with 01:00:5e:

PORT-LIST	Port list, of the form: u[[/s[/p]]][-u[[/s[/p]]][,u[[/s[/p]]]]... Where u, s and p represent a 1- or 2-digit unit number, slot number and port number respectively. You can specify: u for all ports on unit number u; u/s for all ports on slot number s on unit u; u/s/p for port p on slot s on unit u; a hyphenated range (blank spaces are not allowed); a list, separated by commas (blank spaces are not allowed).

Example

```
device-name(config)#ip igmp snooping vlan 1 static 01:00:5e:00:01:29
interface 1/1/1,1/1/4-1/1/8
```

ip igmp snooping vlan immediate-leave

The **ip igmp snooping vlan immediate-leave** command, in Global Configuration mode, enables IGMP Immediate-Leave Processing on the VLAN interface. The **no** form of this command disables Immediate-Leave processing.

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an *IGMP version 2 leave* message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.

Command Syntax

```
device-name(config)#ip igmp snooping vlan <vlan-id> immediate-leave
device-name(config)#no ip igmp snooping vlan <vlan-id> immediate-leave
```

Argument Description

vlan-id	<1-4094> VLAN id value

Example

```
device-name(config)#ip igmp snooping vlan 1 immediate-leave
```

ip igmp snooping for-all

The **ip igmp snooping for-all** command, in Global Configuration mode, enables forwarding of the entire multicast traffic via the specified port list. By default, forwarding is disabled. To remove the port list, use the **no** form of this command.

Command Syntax

```
device-name(config)#ip igmp snooping for-all PORT-LIST
device-name(config)#no ip igmp snooping for-all PORT-LIST
```

Argument Description

PORT-LIST	Port list, of the form u[[/s[/p]]][-u[[/s[/p]]][,u[[/s[/p]]]]]... Where u, s and p represent a 1- or 2-digit unit number, slot number and port number respectively. You can specify: • u for all ports on unit number u; • u/s for all ports on slot number s on unit u; • u/s/p for port p on slot s on unit u; • a hyphenated range (blank spaces are not allowed); • a list, separated by commas (blank spaces are not allowed).

Example

```
device-name(config)#ip igmp snooping for-all 1/1/1-1/1/5
```

ip igmp snooping forbidden

The **ip igmp snooping forbidden** command, in Global Configuration mode, forbids forwarding of the entire multicast traffic via the specified port list. By default, the command is disabled. To remove the port list, use the **no** form of this command.

Command Syntax

```
device-name(config)#ip igmp snooping forbidden PORT-LIST
device-name(config)#no ip igmp snooping forbidden PORT-LIST
```

Argument Description

PORT-LIST	Port list, of the form u[[/s[/p]]][-u[[/s[/p]]][,u[[/s[/p]]]]]... Where u, s and p represent a 1- or 2-digit unit number, slot number and port number respectively. You can specify: • u for all ports on unit number u; • u/s for all ports on slot number s on unit u; • u/s/p for port p on slot s on unit u; • a hyphenated range (blank spaces are not allowed); • a list, separated by commas (blank spaces are not allowed).

Example

```
device-name(config)#ip igmp snooping forbidden 1/1/1-1/1/5
```

ip igmp snooping router-timers

The **ip igmp snooping router-timers** command, in Global Configuration mode, enables you to configure the query packet intervals sent to the host port when performing *leave* snooping. The command sets the Multicast router timer variables (described in RFC 2236) to synchronize the IGMP snooping.

By default – when the switch receives a leave packet from a host that is a member of a certain group, it perform the following:

1. Sends a specific query for that group, with the response time field set to 10 seconds.
2. Waits 120 seconds
3. If no join packet is received – the switch sends a specific query for that group with the response time field set to 10 seconds.
4. Waits 120 seconds.
5. If no join packet is received - waits10 more seconds.
6. If no join packet is received - sends the leave packet to the Multicast router port .

NOTE  This is done also when Immediate leave is enabled but the host is not the last member of that group.

Command Syntax

```
device-name(config)#ip igmp snooping router-timers {query <1-65535>|
responses <responses-value>|robustness  <robustness-value>}
```

Argument Description

query <1-65535>	The time interval, in seconds, between two specific queries. The default value is 120 seconds. The range is <1-65535>.
responses <responses-value>	The expected response time, in seconds, for answering a specific query. The default value is 10 seconds. The range is <1-125>. This value will be inserted in the response-time field of the specific query packet generated by the switch. The response time must be greater than zero and less than the query interval.
robustness <robustness-value>	The number of specific query packets sent by the switch. The default value is 2. Any number higher then 1 is a valid value.

Example

```
device-name(config)#ip igmp snooping router-timers query 30
Query interval is 30 sec
device-name(config)#ip igmp snooping router-timers responses 55
device-name(config)#ip igmp snooping router-timers robustness 7555555
```

Four specific queries will be sent every 30 seconds with response time set to 55 seconds. If no join is received after 220 seconds, the leave packet will be sent to the Multicast router port.

ip igmp snooping send-query

The **ip igmp snooping send-query** command, in Global Configuration mode**,** defines the query generator**.** The query generator can be implemented only when IGMP Snooping is enabled. It generates queries at the configured rate (query-interval). Up to 10 simultaneous queries can be sent. To disable the query generator, use the **no** form of this command.

Command Syntax

```
device-name(config)#ip igmp snooping send-query vlan <vlan-id> interface
PORT-LIST [group A.B.C.D]  [query-interval <query-interval-value>]
[response-time <response-time-value>]
device-name(config)#no ip igmp snooping send-query vlan <vlan-id> interface
PORT-LIST
```

Argument Description

vlan <vlan-id>	Query VLAN tag number in range <1-4094>.
interface PORT-LIST	Query port list distribution.
group A.B.C.D	(Optional) Specifies the group IP (in format A.B.C.D) to which to generate query. The query may be specific or general. By default, all Router Query (224.0.0.1)
query-interval <query-interval-value>	(Optional) Specifies the interval between queries in seconds, in the range <1-300>. By default the value is 120 seconds.
response-time <response-time-value>	(Optional) Specifies the host response timeout, in seconds, to set the query frame, in the range <1-25>. By default the value is 10 seconds.

NOTE The configured response timeout value is specified in seconds, but the value inserted in the packet is in 1/10 second units.

Example

The following example shows how to set the general query packet every 5 seconds in VLAN 5 interface 1/1/1 with response timeout of 15 seconds:

```
device-name(config)#ip igmp snooping send-query vlan 5  interface 1/1/1
query-interval 5 response-time 15
```

Commands to Display IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

show ip igmp snooping

The s**how ip igmp snooping** command, in Privileged (Enable) mode, displays snooping configuration information for the switch or for a specified VLAN.

Command Syntax

```
device-name#show ip igmp snooping [vlan vlan-id]
```

Argument Description

vlan-id	(Optional) <1-4094> VLAN id value

Example

```
device-name#show ip igmp snooping
vlan 1
===
IGMP snooping is globally enabled.
IGMP snooping is enabled on this VLAN.
IGMP snooping immediate-leave is disabled on this Vlan.
 Group Addr      Port   Vid  Age  Type
235.80.68.83     1/1/1    1  108 { REPORTv2 }
 Group Addr             Vid       Ports

235.80.68.83              1    0  | 1/1/1
```

show ip igmp snooping mrouter

The **show ip igmp snooping mrouter** command, in Privileged (Enable) mode, displays information on dynamically learned and manually configured multicast router interfaces.

Command Syntax

```
device-name#show ip igmp snooping mrouter [vlan <vlan-id>]
```

Argument Description

vlan <vlan-id>	(Optional) ID of VLAN for which information is displayed. If this argument is not specified, information for all VLANs is displayed.

Example

The following example displays static and dynamic multicast router interfaces for all VLANs.

```
device-name#show ip igmp snooping mrouter

 vlan | port | static/dynamic
------+----+-------------------
0001 | 1/1/2| static
0001 | 1/1/1| dynamic
```

show ip igmp snooping router-timers

The **show ip igmp snooping router-timers** command, in Privileged (Enable) mode, displays the multicast router timers parameters.

Command Syntax

```
device-name#show ip igmp snooping router-timers [query|responses|
robustness]
```

Argument Description

query	Displays the time interval, in seconds, between two specific queries.
responses	Displays the expected response time, in seconds, for answering a specific query.
robustness	Displays the number specific query packets sent by the switch.

Example

The following example displays static and dynamic multicast router interfaces for all VLANs.

```
device-name#show ip igmp snooping router-timers query
Query interval is 30 sec
device-name#show ip igmp snooping router-timers responses
Responses interval is 15 sec
device-name#show ip igmp snooping router-timers robustness
Robustness = 4 packets
```

show ip igmp snooping send-query

The **show ip igmp snooping send-query** command, in Privileged (Enable) mode, displays the query generator information.

Command Syntax

```
device-name#show ip igmp snooping send-query
```

Example

```
device-name#show ip igmp snooping send-query
Responses interval is 15 sec
```

show mac-address-table multicast igmp

The **show mac-address-table multicast igmp** command, in Privileged (Enable) mode, displays MAC address table entries for a VLAN.

Command Syntax

```
device-name#show mac-address-table multicast igmp [vlan <vlan-id>] [count]
```

Argument Description

vlan <vlan-id>	(Optional) The multicast group VLAN ID.
count	(Optional) Displays only the total number of entries for the selected criteria, not the actual entries.

Example

The following example displays all the MAC address table entries for VLAN 1.

```
device-name#show mac-address-table multicast igmp vlan 1
```

```
vlan___|__mac_address_______|_type_____|ports_____________
0001     01:00:5e:00:00:00   user       1/1/2
0001     01:00:5e:00:00:00   igmp      1/1/5
0001     01:00:5e:00:01:29   igmp      1/1/2,1/1/4,1/1/5,1/1/8
0001     01:00:5e:11:11:11   user       1/1/1,1/1/3
0001     01:00:5e:11:11:11   igmp      1/1/2
device-name#show mac-address-table multicast igmp count
multicast mac entries : 5
device-name#show mac-address-table multicast igmp vlan 1 count
multicast mac entries for vid 1 : 5
```

Commands to Show and Clear IGMP Statistics Counters

To display the IGMP Statistics Counters use the following commands.

show ip igmp statistics

The **show ip igmp statistics** command, in Privileged (Enable) mode or in global Configuration mode, displays the current settings of various IGMP Statistics Counters, according to the specified parameter.

Command Syntax

```
device-name#show ip igmp snooping statistics <parameter>
```

Argument Description

groups	Number of simultaneous groups
leaves	Number of leave packets received
ports	Number of ports registered (per VLAN per group) simultaneously
queries	Number of query packets received
reports	Number of report packets received

clear ip igmp snooping

The **clear ip igmp snooping** command, in Privileged (Enable) mode, clears all (if no parameter is configured) or specified IGMP Counters.

Command Syntax

```
device-name#clear ip igmp snooping [parameter]
```

Argument Description

groups	Clears the simultaneous groups counter

leaves	Clears the leave packets received counter
ports	Clears the registered ports counter
queries	Clears the query packets received counter
reports	Clears the report packets received counter

21. Multicast VLAN Registration (MVR)

Introduction

MVR (Multicast VLAN Registration) is designed to serve two purposes:

- To enable efficient, secure multicast data flow across VLANs in a simple configuration.
- To support dynamic join to multicast groups, in order to enable channel zapping.

This will allow you to support multicast services, while keeping the user security provided by the VLAN and features. Users on different VLANs cannot exchange any information between them, but multicast services are provided.

A maximum of 256 MVR multicast groups can be configured on a switch.

Any multicast data sent to a configured multicast address is sent to all receiver ports that have registered to receive data on that multicast address, even if the source and receiver ports are on different VLANs.

The device can force the multicast server to send all the configured multicast frames to the switch, to allow quick zapping.

NOTES

1. To enable MVR, you must first enable IGMP snooping, using the ip igmp snooping command, described in IGMP Snooping Commands.
2. The IP address range from 224.0.0.0 to 239.255.255.255 is reserved for multicast host groups.

An example of an MVR configuration is shown in Figure 21-1.

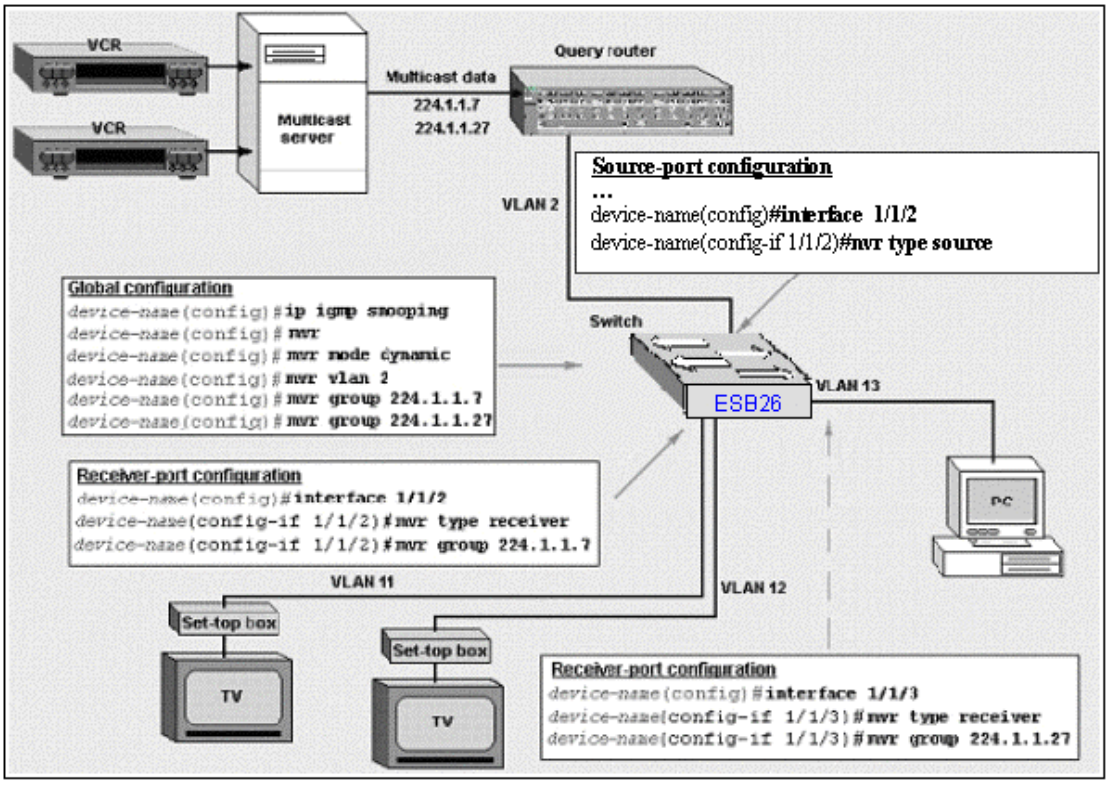


Figure 21-1 Example of an MVR Configuration

This setup allows cross-VLAN multicast frames to be sent from VLAN 2 to users on other VLANs through registered receiver ports.

Description of Commands

MVR Global Configuration Commands

Table 21-1 summarizes the MVR configuration commands available in global Configuration mode.

Table 21-1 MVR Global Configuration Commands

Command	Description
mvr	Enables MVR. The no form of this command disables MVR.
mvr mode	Specifies whether the mode of operation is static or dynamic.
mvr group	Statically configures an MVR group IP multicast address or a sequence of MVR group IP multicast addresses on the switch.
mvr querytime	Sets the maximum time to wait for IGMP report memberships on a receiver port.
mvr vlan	Specifies the VLAN on which MVR multicast data is expected.

mvr

The **mvr** command, in Global Configuration mode, enables MVR. The **no** form of this command disables MVR.

By default, MVR is disabled.

When you disable MVR, the entire MVR configuration is erased.

Command Syntax

```
device-name(config)#mvr
device-name(config)#no mvr
```

Example

See the examples below.

mvr mode

The **mvr mode** command, in Global Configuration mode, specifies the mode of operation, either **static** or **dynamic**.

The default MVR mode is **dynamic**.

Command Syntax

```
device-name(config)# mvr mode dynamic|static [group A.B.C.D [<count>]]
[querytime <value>][vlan <vlan-id>]

device-name(config)#mvr mode static [vlan <vlan-id>]
```

Argument Description

dynamic	The switch forces the multicast server to send all configured multicast-group data to the source port, without waiting for join requests from receiver ports. When a user on a receiver port sends a join to a multicast group, it immediately starts receiving the multicast data. The response to joins and channel zapping is quick, at the expense of loading the switch with traffic from all the configured multicast groups all the time. If no multicast group is defined the default will be 224.0.0.1. Under normal conditions, dynamic mode is preferable.
static	Multicast data is sent only after a request has been sent from a receiver port to join that multicast group. The response in this mode is slower than the response in dynamic mode, but the switch is not loaded with traffic from unused multicast groups.
vlan vlan-id	ID of the VLAN on which MVR multicast data is expected in range <1-4094>. The default VLAN ID is 1.
A.B.C.D	The IP multicast address of the MVR group.
count	(Optional) Configures multiple contiguous MVR group addresses. The default is 1. The allowed range is <1-256>.
value	The response time in seconds. The default is 10 seconds. The allowed range is <1-25> seconds.

Example

See the examples below.

mvr group

The **mvr group** command, in Global Configuration mode, statically configures an MVR group IP multicast address on the switch.

The **no** form of this command, with an IP address specified, removes the specified statically configured IP multicast. If no IP address is specified, the **no** form of this command removes all statically configured MVR IP multicast addresses.

By default, no IP multicast addresses are configured on the switch. The default group IP address count is 1.

Use the **mvr group** command to statically set up all the IP multicast addresses that will take part in MVR.

Command Syntax

```
device-name(config)#mvr group A.B.C.D [<count>]
device-name(config)#no mvr group [A.B.C.D]
```

Argument Description

A.B.C.D	The IP multicast address of the MVR group.
count	(Optional) Configure multiple contiguous MVR group addresses. The default is 1. The allowed range is 1-256.

Example

See the examples below.

mvr querytime

The optional **mvr querytime** command, in Global Configuration mode, sets the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-ports and affects leave processing. When an IGMP query is sent to a receiver port, the switch waits for the default or configured MVR query-time for an IGMP group membership report before removing the port from multicast group membership.

This command overrides the query response time indicated in the IGMP query packets received from the query router.

The **no** form of this command restores the default setting of 10 seconds.

NOTE  The mvr querytime command is relevant only in dynamic mode.

Command Syntax

```
device-name(config)#mvr querytime <value>
device-name(config)#no mvr querytime
```

Argument Description

value	The response time in seconds. The default is 10 seconds. The allowed range is 1-25 seconds.

Example

See the examples below.

mvr vlan

The **mvr querytime** command, in Global Configuration mode, specifies the ID of the VLAN on which reception of MVR multicast data is expected (the source-port VLAN ID).

The default multicast VLAN ID for MVR is 1.

Command Syntax

```
device-name(config)#mvr vlan <vlan-id>
```

Argument Description

vlan-id	ID of the VLAN on which MVR multicast data is expected. The range is <1-4094>, and the default VLAN ID is 1.

Examples

1. The following example shows how to enable MVR. Before using the **mvr** command, make sure that IGMP snooping is enabled.

```
device-name(config)#ip igmp snooping
device-name(config)#mvr
```

2. The following example shows how to disable MVR:

```
device-name(config)#no mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

3. The following example shows how to configure 228.1.23.4 as an IP multicast address:

```
device-name(config)#mvr group 228.1.23.4
```

4. The following command fails because of address aliasing:

```
device-name(config)#mvr group 230.1.23.4
Cannot add this IP address - aliases with previously configured IP address
228.1.23.4.
```

5. The following example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
device-name(config)#mvr group 228.1.23.1 10
```

6. The following example shows how to delete the previously configured IP multicast

address:

```
device-name(config)#no mvr group 228.1.23.1
```

7. The following example shows how to delete all previously configured IP multicast addresses:

```
device-name(config)#no mvr group
```

8. The following example shows how to set the maximum query response time to 15 seconds:

```
device-name(config)#mvr querytime 15
```

9. The following example shows how to reset the maximum query response time to the default setting 10 seconds:

```
device-name(config)#no mvr querytime
```

10. The following example shows how to set VLAN 2 as the multicast VLAN:

```
device-name(config)#mvr vlan 2
```

MVR Interface Configuration Commands

Table 21-2 summarizes the MVR configuration commands available in Interface Configuration mode.

Table 21-2 MVR Interface Configuration Commands

Command	Description
mvr type	Configures the port either as an MVR receiver port or as a source port.
mvr immediate	Enables or disables the Immediate Leave feature of MVR on a port.
mvr group	Statically configures the specified MVR group IP multicast address for the specified VLAN ID.
no mvr	Removes the configured port from the MVR ports list.

mvr type

The **mvr type** command, in Interface Configuration mode, configures the port either as an MVR receiver port or as a source port.

Command Syntax

```
device-name(config-if UU/SS/PP)#mvr type {source|receiver}
```

Argument Description

source	Configures the port as an uplink port that can receive multicast data for the configured multicast groups. There can be more than one source port in a switch.

	See the Note below.
receiver	Configure the port as a subscriber port that can receive multicast data.

NOTE

1. If mvr type is not specified, this port is a receiver port.
2. If the queries and the multicast data are received from different ports, configure the port from which the queries are received as the source port.

Example

See the examples below.

mvr immediate

The **mvr immediate** command, in Interface Configuration mode, enables the Immediate Leave feature of MVR on a port. The **no mvr immediate** command disables the feature.

By default, the Immediate Leave feature is enabled on all ports.

Command Syntax

```
device-name(config-if UU/SS/PP)#mvr immediate
device-name(config-if UU/SS/PP)#no mvr immediate
```

Example

See the examples below.

mvr group

The **mvr group** command, in Interface Configuration mode, configured on receiver ports, statically configures the specified MVR group IP multicast address for the specified VLAN ID. This is the IP address of the multicast group that the port is allowed to join.

The **no** form of this command, with an IP address specified, removes the configured port from membership in the specified IP multicast address group. If no IP address is specified, the **no** form of this command removes the configured port from membership in all configured multicast groups.

By default (if this command is not used), no IP address will be allowed to join the multicast group.

If the command is used without specifying an IP address – all groups are allowed to join.

Command Syntax

```
device-name(config-if UU/SS/PP)#mvr group [A.B.C.D]
device-name(config-if UU/SS/PP)#no mvr group [A.B.C.D]
```

Argument Description

A.B.C.D	(Optional) MVR group IP multicast address.

Example

See the examples below.

no mvr

The **no mvr** command, in Interface Configuration mode, removes the MVR configuration from the specified port.

Command Syntax

```
device-name(config-if UU/SS/PP)#no mvr
```

Examples

1. The following example shows how to configure port 1/1/1 as an MVR receiver port:

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#mvr type receiver
```

2. The following example shows how to configure Ethernet port 1/1/1 as an MVR source port:

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#mvr type source
```

3. The following example shows how to remove port 1/1/1 as an MVR port:

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#no mvr group
```

MVR Show Commands

Table 21-3 summarizes the MVR show commands.

Table 21-3 MVR Show Commands

Command	Description
show mvr	Displays configured MVR parameters with regard to the switch.
show mvr interface	Lists the current MVR configurations and status per MVR ports.
show mvr members	Lists the current MVR configurations and status per MVR groups.

show mvr

The **show mvr** command, in Privileged (Enable) mode, displays the following information, with regard to the switch:

- MVR status (enabled or disabled)

- MVR multicast vlan ID
- Maximum number of MVR multicast groups
- Current number of MVR multicast groups
- Current MVR Query response time (configured or received online from the query router)
- Configured MVR mode (Static or Dynamic)

Command Syntax

```
device-name#show mvr
```

Example

```
device-name#show mvr
MVR Status: enable
MVR multicast vlan: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 256
MVR Global query response time: 5
MVR Mode: Dynamic
```

show mvr interface

The **show mvr interface** command, in Privileged (enable) mode, lists the current MVR configurations of the switch's MVR configured ports.

Command Syntax

```
device-name#show mvr interface
```

Example

```
device-name#show mvr interface
=================================================================
 Interface    | Type      | Status         | Immediate Leave
--------------+-----------+----------------+--------------------
 1/1/1        | Receiver  | Active/up      | Enable
 1/1/2        | Receiver  | Inactive/up    | Disable
 1/1/20       | Source    | Active/up      | -
```

show mvr members

The **show mvr members** command, in Privileged (enable) mode, lists the current list of active interfaces per MVR group.

Command Syntax

```
device-name#show mvr members
```

Example

```
device-name#show mvr members
=================================================================
```

```
MVR Group  | Active Interface List
-----------+--------------------------
224.0.0.3    1/1/1, 1/1/2, 1/1/4
224.0.0.4    none
```

22. Transparent LAN Services (TLS)

Introduction

Service providers are discovering significant new revenue opportunities with Layer 2 services that extend customer LANs across geographically dispersed sites. Using metro Ethernet technology, service providers can offer services that connect multiple enterprise customer offices at Ethernet's 10-Mbps up to 1-Gbps LAN speeds.

Deploying these services called "Transparent LAN Services (TLS)" requires network operators to transport a large number of customers' virtual LANs (VLANs) while keeping traffic in each VLAN secured from other customers' VLANs. To do so, they can use the TLS feature, which segregates VLANs in a way that also overcomes management and scalability obstacles.

Large business customers usually create 802.1Q VLANs within their enterprises to segregate certain traffic flows running across their Ethernet inter-networks. They define a certain number of internal VLANs, which act like "Ethernet tunnels," to separate groups of users (the engineering department from the corporate marketing department, for example). Each VLAN supports a population of users with something in common, such as those who share the same set of network access rights.

Service providers can use the TLC feature to offer services that provide the same high-speed, VLAN-based experience that customers enjoy in the LAN across the metropolitan-area network (MAN) and the WAN. The TLC feature adds a VLAN header to the packet with EtherType field that is different from the 802.1Q tag of the customer traffic in the switch at the edge of the service provider's network.

If the switch receives an untagged packet, it adds a tag header to the packet with EtherType that is not the standard EtherType (0x8100). If the switch receives a packet with a tag header, it adds another tag header with EtherType that is not the standard EtherType (0x8100).

Feature Overview

Transparent LAN Services (TLS) implies Layer 2 connectivity offered by a service provider to multiple customer sites in a manner that is transparent to the customer edge (CE) devices.

The switch is positioned on the edge of the provider network. It is connected to customer edge (CE) switches, and interfaces to the provider network.

To provide TLS, Ethernet frames originated by the source CE switch are received at the provider edge (PE) switch, encapsulated and transported across the provider network, where the PE switch removes the encapsulation and delivers the unmodified frame to the destination CE switch (see Figure 22-1).

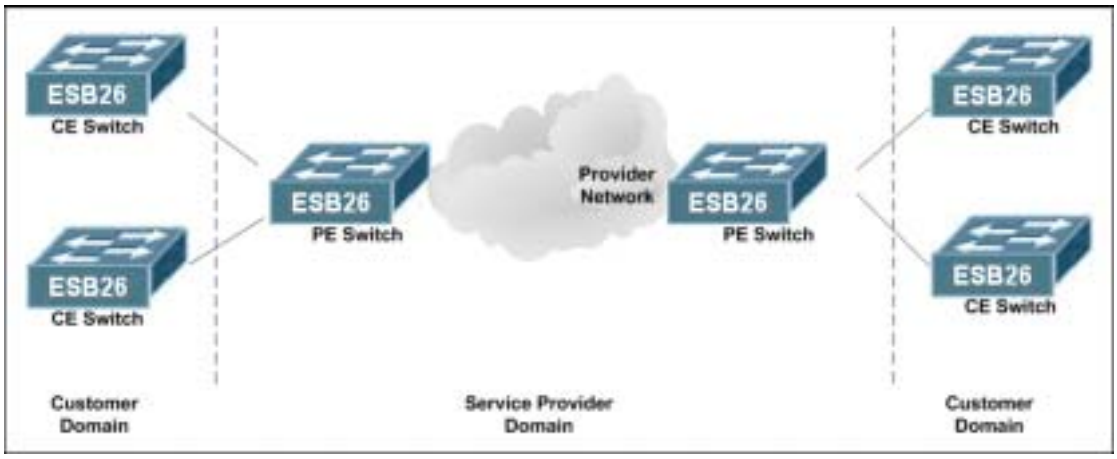


Figure 22-1 Schematic TLS Representation

The 802.1Q VLAN-ID tag (VID) in the user's traffic is transparent to the switches. This allows all the CE switches to behave as if attached to a shared LAN.

Two types of ports are defined in the network switches deployed by the service provider:

- User (customer) port – a port that is connected to a user. Packets that are transmitted through this port have no added tag.
- Uplink (core) port – a port that is connected to the service provider's network. All packets that are transmitted through this port are either control packets or packets with an additional tag.

Jumbo Frame

The Jumbo frame is an extension to current Ethernet Frame specifications for hardware and frame format to support payloads greater than 1500 Bytes for Type interpretation and Length interpretation frames. This is useful for Gigabit Ethernet technology, providing a means to carry large MTU packets without fragmentation over a high-speed broadcast network.

Jumbo frames are used between end-stations that support larger frame sizes for more efficient transfers of bulk data. Both end-stations involved in the transfer must be capable of supporting jumbo frames.

The **tls jumbo-frame** command in Global Configuration mode enables more efficient packet processing on workstations and servers by increasing the maximum packet size to 10K.

Supported Standards, MIBs and RFCs

Standards

No standards are supported by this feature.

MIBs

No MIBs are supported by this feature.

RFCs

No RFCs are supported by this feature.

Prerequisites

When TLS is enabled, the priority classification on the received traffic is disabled and all the packets are assigned the port's default priority. The packet's priority can also be based on the IP ToS field.

The TLS ports must be set on a VLAN. The VLAN number could be any VLAN from the VLAN range <1-4094> as long as the TLS uplink is tagged on this VLAN and the TLS user is untagged on this VLAN.

Default TLS Configuration

Table 22-1 shows the default TLS configuration.

Table 22-1 TLS Default Configuration

Parameter	Default Value
Transparent LAN Services (TLS)	Disabled
EtherType	0x9000
Jumbo frame	Disabled

Configuring and Displaying TLS

Configuring TLS

To set the TLS, proceed as follows:

1. Enable TLS. See Enabling/Disabling the TLS.
2. Set the EtherType if you want settings other than the default. See **Error! Reference source not found.**.
3. Set the uplink ports. See Assigning the TLS Uplink to an Interface.

NOTE By default, all the ports are set as TLS users.

Table 22-2 lists the TLS configuration commands.

Table 22-2 TLS Configuration Commands

Command	Description
tls	Enables/disables TLS on the switch.
tls ethertype	Assigns the EtherType value.
tls uplink	Assigns a TLS uplink to the configured interface.

Enabling/Disabling the TLS

The **tls** command, in Global Configuration mode, enables or disables the TLS on the switch.

NOTE TLS cannot coexist with IGMP Snooping.

Command Syntax

```
device-name(config)#tls {enable | disable}
```

Argument Description

enable	Enables the TLS.
disable	Disables the TLS.

Setting the TLS Ethertype Value

The **tls ethertype** command, in Global Configuration mode, sets the EtherType value. By default, the EtherType value is 0x9000.

NOTE The TLS must be enabled before executing this command. To enable the TLS use the tls enable command in Global configuration mode.

Command Syntax

```
device-name(config)#tls ethertype <number>
```

Argument Description

number	Hexadecimal VLAN EtherType value.

Assigning the TLS Uplink to an Interface

The **tls uplink** command in Interface Configuration mode, assigns the TLS uplink to the configured interface. To remove the TLS uplink, use the **no** form of this command.

The TLS uplink is configured at the Provider-network side of the provider-edge (PE) switch.

Note that the interface remains TLS uplink port until the TLS is globally disabled or changed to TLS user.

NOTE The TLS must be enabled before executing this command. To enable the TLS use the tls enable command in Global configuration mode.

The TLS uplink must be configured as tagged on the TLS VLAN.

Command Syntax

```
device-name(config-if UU/SS/PP)#tls uplink
device-name(config-if UU/SS/PP)#no tls uplink
```

Displaying TLS Configuration

Table 22-3 lists the TLS displaying commands.

Table 22-3 TLS Displaying Commands

Command	Description
show tls	Displays the global TLS configuration.

Displaying the TLS Configuration

The **show tls** command, in Privileged (Enable) mode, displays the TLS configuration:

- The TLS status
- The TLS EtherType
- The TLS uplink ports

Command Syntax

```
device-name#show tls
```

Example

```
device-name#show tls
TLS is enabled

TLS EtherType 0x7000
interface 1/2/1 TLS uplink
```

Jumbo Frame Commands

Table 22-4 Jumbo Frame Commands lists the jumbo frame configuring and displaying commands.

Table 22-4 Jumbo Frame Commands

Command	Description
tls jumbo-frame	Enables jumbo frame.
show tls jumbo-frame	Displays the jumbo frame status.

Enabling Jumbo Frames

The **tls jumbo-frame** command, in Global Configuration mode, allows support of large (10K) frames. The no form of the command restores the packet buffer size to its default settings (1518 bytes).

The **tls jumbo-frame** command enables more efficient packet processing on workstations and servers by increasing the maximum packet size to 10K.

Jumbo frames are frames larger than the standard Ethernet frame size, which is 1518 bytes (including Layer 2 header and Frame Check Sequence (FCS)).

The default MTU size is also 10K bytes once jumbo frame support has been enabled.

NOTE

1. The tls jumbo-frame command will take effect only after reset. You need not save the configuration for the jumbo frame to take effect.
2. The tls jumbo-frame command will not appear in the configuration file.

Command Syntax

```
device-name(config)#tls jumbo-frame
device-name(config)#no tls jumbo-frame
```

Displaying the Jumbo-Frame Configuration Status

The **show tls jumbo-frame** command, in Privileged (Enable) mode, displays the jumbo frame configuration status.

Command Syntax

```
device-name#show tls jumbo-frame
```

Example

```
device-name#show tls jumbo-frame
tls Jumbo frame is on
```

Configuration Example

Figure 22-2 shows an example of an interface TLS configuration. The configuration for the PE switches is the same. In this example, the users cannot communicate with each other.

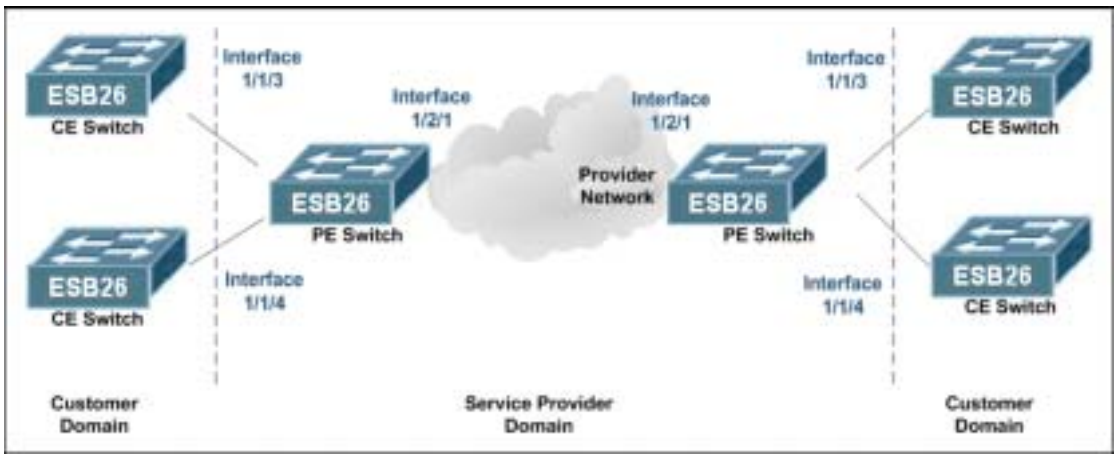


Figure 22-2 TLS Interface Example

1. Enable TLS:

```
device-name#configure terminal
device-name(config)#tls enable
```

2. Set the EtherType to 0x7000:

```
device-name(config)#tls ethertype 7000
```

3. Set the TLS uplink on interface 1/2/1:

```
device-name(config)#interface 1/2/1
device-name(config-if 1/2/1)#tls uplink
```

4. Add the TLS uplink as user in VLAN *default* (VLAN ID 1). Note that the TLS user is a member in VLAN 1 by default.

```
device-name(config)#vlan
device-name(config vlan)#config default
device-name(config-vlan default)#add ports 1/1/1 tagged
device-name(config-vlan default)#end
```

5. Display the TLS configuration:

```
device-name#show tls
TLS is enabled
TLS EtherType 0x7000

interface 1/2/1 TLS uplink
```

23. Software Upgrade and Reboot Options

Overview

The following kinds of commands are discussed in this chapter:

- **Copy** commands – These commands allow you to download or save startup and running configurations.
- **Write** commands – These commands allow you to display information on the current configuration, store the current configuration on the switch's NVRAM, or reload the factory-default configuration settings.
- **Reload** commands – These commands allow you to reboot the switch with or without saving the current configuration, or reload the factory-default configuration settings.
- **Show** commands – These commands display information regarding the switch configuration settings.

Note that each **write** command has an alias (or nearly alias) **copy**, **reload** or **show** command.

Description of Commands

Copy Commands

The **Copy** commands, summarized in Table 23-1, perform the following operations:

- Download new software versions to the switch.
- Save or load the start-up configuration.
- Save the start-up configuration as the running configuration.

Table 23-1 Copy Commands

Command	Description
copy application	Downloads a new software version to the switch.
copy startup-config download-from	Loads a start-up configuration with the specified file name from a remote server with the specified IP address.
copy startup-config upload-to	Saves the start-up configuration on the remote server with the specified IP address to the specified file name.
copy running-config startup-config	Saves the running-configuration as the startup configuration. The command is equivalent to the write memory command.

Command	Description
copy running-config download-from	Loads a running-configuration with the specified file name, from a remote server with the specified IP address.
copy running-config upload-to	Saves the running configuration on the remote server with the specified IP address to the specified file name.
copy sysloader	Downloads a new sysloader version to the switch
swap application	Swaps the primary and secondary applications

copy application

The **copy application** command, in Privileged (Enable) mode, downloads a new software version to the switch.

The image file contains the executable code that runs on the switch. It comes preinstalled from the factory. As new versions of the image are released, you should upgrade the software that is running on your system. The image is upgraded by using a download procedure from a TFTP server on the network.

The primary application becomes secondary and stores the new image as a primary when you use the option **leave-primary-sw**.

For more information about the dual boot feature, primary and secondary application of the switch, refer to the "System Lodaer" chapter.

Command Syntax

```
device-name#copy application (primary|secondary|leave-primary-sw)
A.B.C.D SOURCE_FILE
```

Argument Description

primary	Copies the image to the primary (first) flash.
secondary	Copies the image to the secondary (second) flash.
leave-primary-sw	Moves the application from the first flash to the second and stores a new image on it.
A.B.C.D	The IP address of the TFTP server.
SOURCE_FILE	The path and name of the source-file (located on the TFTP server). Note that the path specification and any file-name limitations may depend on the software running on the TFTP server.

NOTE Both images (the primary and the secondary) should be dual boot images.

Example

The following command downloads the new software-version file named **VER*123*** located on C:/ on the TFTP server at IP address 192.192.54.0 and saves it as a primary application.

```
device-name#copy application primary 192.192.54.0 c:/VER123
```

copy startup-config download-from

The **copy startup-config download-from** command, in Privileged (Enable) mode, loads a start-up configuration specified by file name from a remote server specified by IP address.

Command Syntax

```
device-name#copy startup-config download-from A.B.C.D SOURCE_FILE
```

Argument Description

A.B.C.D	The IP address of the TFTP server.
SOURCE_FILE	The path and name of the source file on the TFTP server. Note that the path specification and any file-name limitations may depend on the software running on the TFTP server.

Example

The following command downloads the start-up configuration file named ***START001*** located on C:/ on the TFTP server at IP address 192.192.54.0.

```
device-name#copy startup-config download-from 192.192.54.0 c:/START001
```

copy startup-config upload-to

The **copy startup-config upload-to** command, in Privileged (Enable) mode, saves the start-up configuration on the remote server with the specified IP address to the specified file name.

Command Syntax

```
device-name#copy startup-config upload-to A.B.C.D TARGET_FILE
```

Argument Description

A.B.C.D	The IP address of the TFTP server.
TARGET_FILE	The path and name given to the target file on the TFTP server. Note that the path specification and any file-name limitations may depend on the software running on the TFTP server.

Example

The following command uploads the start-up configuration to a new file named ***START002***, on C:/ on the TFTP server at IP address 192.192.54.0.

```
device-name#copy startup-config upload-to 192.192.54.0 c:/START002
```

copy running-config startup-config

The **copy running-config startup-config** command, in Privileged (Enable) mode, saves the running-configuration as the startup configuration. This is the configuration that will be saved and loaded each time power to the unit is turned on.

The command is equivalent to the **write memory** command.

Command Syntax

```
device-name#copy running-config startup-config
```

copy running-config download-from

The **copy running-config download-from** command, in Privileged (Enable) mode, loads a running-configuration with the specified file name, from a remote server with the specified IP address.

The commands from the downloaded running-configuration are executed and the result is a merge between the previous running-configuration and the current switch configuration.

Command Syntax

```
device-name#copy running-config download-from A.B.C.D CONFIG_FILE
```

Argument Description

A.B.C.D	The IP address of the TFTP server.
CONFIG_FILE	The path and name of the source file located on the TFTP server. Note that the path specification and any file-name limitations may depend on the software running on the TFTP server.

Example

The following command downloads the running-configuration file named ***RUN001*** located on C:/ on the TFTP server at IP address 192.192.54.0.

```
device-name#copy running-config download-from 192.192.54.0 c:/RUN001
```

copy running-config upload-to

The **copy running-config upload-to** command, in Privileged (Enable) mode, saves the running configuration to the specified file on the remote server at the specified IP address.

Command Syntax

```
device-name#copy running-config upload-to A.B.C.D TARGET_FILE
```

Argument Description

A.B.C.D	The IP address of the TFTP server.

TARGET_FILE	The path and name given to the target file on the TFTP server. Note that the path specification and any file-name limitations may depend on the software running on the TFTP server.

Example

The following command uploads the running-configuration to a new file named *RUN002*, on C:/ on the TFTP server at IP address 192.192.54.0.

```
device-name#copy startup-config upload-to 192.192.54.0 c:/RUN002
```

copy sysloader

The **copy sysloader** command, in Enable mode, copies the system loader.

Command Syntax

```
device-name# copy sysloader A.B.C.D FILE-NAME
```

Argument Description

A.B.C.D.	The IP address of the TFTP server.
FILE-NAME	The path and name of the source-file (located on the TFTP server). Note that the path specification and any file-name limitations may depend on the software running on the TFTP server.

NOTE

Update of Sysloader software should be done only by instruction of Technical Support. Powering down the switch in during sysloader save can prevent the switch from being able to startup.

swap application

The **swap application** command, in Enable mode, swaps the primary and secondary applications.

Command Syntax

```
device-name# swap application
```

Write Commands

The **Write** commands, summarized in Table 23-2, can be used to perform the following operations:

- Display detailed information regarding the current configuration of the unit on the terminal monitor;

- Reload factory-default configuration settings;
- Store the unit's current configuration on the NVRAM of the switch.

Table 23-2 Write Commands

Command	Description
write terminal	Displays detailed information regarding the current configuration of the unit on the terminal monitor. The command is equivalent to the show running-config command.
write erase	Resets the current configuration of the unit stored on the NVRAM of the switch. The start-up configuration file is set to factory-default values. This command is similar to reload to-defaults, except that it does not restart the switch.
write memory	Stores the unit's current configuration on the NVRAM of the switch. The command is equivalent to the copy running-config startup-config command.

write terminal

The **write terminal** command, in Privileged (Enable) mode, displays detailed information regarding the current configuration of the unit on the terminal monitor.

The command is equivalent to the **show running-config** command.

Command Syntax

```
device-name#write terminal
```

Example

```
device-name#write terminal
building the configuration ...
! current configuration:
!
! version 3.5.9.2 $revision: 1.110 $
!
...
```

Further information displayed includes the following:

- IP Address
- SNMP Server Configuration
- Web-Server Configuration
- Protocol Configuration
- Port Configuration
- All Connected Interfaces
- QoS Configuration
- Resilient Link Configuration
- VLAN Configuration
- IGMP And Multicast Configuration

write erase

The **write erase** command, in Privileged (Enable) mode, erases the current configuration of the unit stored on the NVRAM of the switch. The start-up configuration file is set to factory-default values.

This command is similar to **reload to-defaults**, except that it does not restart the switch.

Command Syntax

```
device-name#write erase
```

write memory

The **write memory** command, in Privileged (Enable) mode, stores the unit's current configuration on the NVRAM of the switch. This is the configuration that will be saved and loaded each time the power to the unit is turned on. The **write** command in Privileged (Enable) mode has the same functionality.

The command is equivalent to the **copy running-config startup-config** command.

Command Syntax

```
device-name#write memory
```

Reload Commands

The **Reload** commands, summarized in Table 23-3, can be used to perform the following operations:

- Reboot the switch, with or without saving the current configuration;
- Reload factory-default configuration settings.

The **reload** commands are available in Privileged (Enable) mode.

Table 23-3 Reload Commands

Command	Description
reload	Closes down and reboots the switch with or without saving the current configuration. Resets the interface modules.
reload to-defaults	Resets the switch to its factory-default configuration and reboots it.
boot-mode	Configures the boot mode.

reload

The **reload** command, in Privileged (Enable) mode, with the optional **save** keyword, saves the current configuration to the NVRAM, resets the interface modules and reboots the switch. Used with the **no-save** keyword, this command closes down and reboots the switch without

saving the current configuration to the NVRAM. When used without arguments, the command functions as the **reload save** command.

When you use the **reload** command, the software requests confirmation before it closes down.

Command Syntax

```
device-name#reload [save|no-save]
```

Argument Description

save	(Optional). Save the running configuration definitions. This is the default.
no-save	Do not save the running configuration definitions.

Examples

1. Saving the current configuration and rebooting the switch (the **save** keyword is optional):

```
device-name#reload save
save current configuration and reboot the switch ? [y/n]: y
Rebooting ...
```

2. Rebooting the switch without saving the current configuration:

```
device-name#reload no-save
Proceed with reload ? [y/n] : y
Rebooting ...
```

reload to-defaults

The **reload to-defaults** command, in Privileged (Enable) mode, resets the switch to its factory-default configuration and reboots it.

Command Syntax

```
device-name#reload to-defaults
```

boot mode

The **boot-mode** command, in Global Configuration mode, sets the boot mode to primary, secondary or auto.

By default, the boot mode is primary.

Command Syntax

```
device-name(config)# boot-mode (primary|secondary|auto)
```

Argument Description

primary	Boots the image from the first flash
secondary	Boots the image from the secondary flash

auto	Starts first the primary application and if it fails the second application is activated. If both applications fail to start, the device enters the Sysloader CLI.

Show Commands

The **Show** commands, summarized in Table 23-4, can be used to:

- Display the current configuration settings.
- Display the saved configuration settings.

The following commands display information regarding the switch configuration settings.

Table 23-4 Show Commands

Command	Description
show startup-config	Displays the switch configuration saved to NVRAM.
show running-config	Displays current run-time information regarding the configuration of the switch. The command is equivalent to the write terminal command.
show boot-mode	Displays the configured boot mode.

show startup-config

The **show startup-config** command, in Privileged (Enable) mode, displays the switch configuration saved to NVRAM (configured information that is saved when the power to the switch is turned off).

Command Syntax

```
device-name#show startup-config
```

Example

```
device-name#show startup-config
! NVRAM Configuration:
!
! ESB26 Version 3.3.0
!
...
```

Further information displayed includes the following:

- IP Address
- SNMP Server Configuration
- Web-Server Configuration
- Protocol Configuration
- Spanning-tree mode (enable/disable)
- VLAN Configuration

- IGMP And Multicast Configuration
- Port configuration

show running-config

The **show running-config** command, in Privileged (Enable) mode, displays information regarding the updated run-time configuration of the switch.

The command is equivalent to the **write terminal** command.

Command Syntax

```
device-name#show running-config
```

Example

```
device-name#show running-config
building the configuration ...
! current configuration:
!
! ESB26 Version 3.3.0
!
...
```

Further information displayed includes the following:

- IP Address
- SNMP Server Configuration
- Web-Server Configuration
- Protocol Configuration
- Spanning tree enable/disable
- VLAN Configuration
- Monitor Session configuration
- IGMP And Multicast Configuration
- Port configuration

show boot-mode

The **show boot-mode** command, in Enable mode, displays the configured boot mode.

Command Syntax

```
device-name# show boot-mode
```

Example

```
device-name# show boot-mode
Boot mode is primary
```

24. File System for Configuration Script Files

Introduction

A script file is a text file that includes a sequence of CLI configuration commands. The ESB26 file system contains a collection of configuration script files. You can also write your own script files, using a text editor.

You can perform the following actions with script files:

- Download script files from the TFTP server;
- Upload script files to the TFTP server;
- Delete script files from the file system;
- Rename script files;
- Run script files;
- View the contents of script files.

Script files are stored in the ESB26 file system. You can show a list of the files stored in the file system, and you can clean the entire file system.

The **reload to-defaults** command (in Privileged mode - clears system data from NVRAM and reboots) does not affect the contents of the file system.

When you run a script file, the current running configuration of the switch is merged with the new settings that are configured by the script file.

The number of configuration script files that you can store is limited only by the storage space available in the switch's file system - 64 KB.

Every file in the file system has a unique name of up to 32 characters without blank spaces.

Script-File Commands

Table 24-1 summarizes the commands available for manipulating and displaying configuration script files.

Table 24-1 Script File Commands

Command	Description
script-file-system	Accesses script file system configuration mode.
copy-from running-config	Copies the running configuration to the script file system.
copy-from startup-config	Copies the startup configuration to the script file system.

Command	Description
delete	Deletes the specified file from the file system.
dir	Displays the names and lengths of all files in the script file system. This command is an alias of the show script file system command.
display	Displays the textual contents of the specified script file.
download-from	Downloads a file from the TFTP server to the file system.
format file-system	Initializes the script file system for the first time.
rename	Renames the specified script file.
run	Executes the CLI commands contained in the specified script file.
show script-file-system	Displays the names and lengths of all files in the script file system. This command is an alias of the dir command, but may be also used in View and Privileged modes.
upload-toscp	Uploads a file from the file system to the TFTP server.Secure copy.

Description of Commands

script-file-system

The **script-file-system** command, in Global Configuration mode, accesses script file system configuration mode.

Command Syntax

```
device-name(config)#script-file-system
```

copy-from running-config

The **copy-from running-config** command, in Script-file-system Configuration mode, copies the running configuration into the specified file. If a file name is not specified, the command copies the running configuration into a file with a default name (***running-config***), created in the script file system.

Command Syntax

```
device-name(config script-file-system)#copy-from running-config [DEST-FILE]
```

Argument Description

DEST-FILE	(Optional) The name of the destination file, in the script file system.

Example

```
device-name(config script-file-system)#copy-from running-config
building the configuration ...
```

```
saving script file "running_config" to file system...  done
```

copy-from startup-config

The **copy-from startup-config** command, in Script-file-system Configuration mode, copies the startup configuration into the specified file. If a file name is not specified, the command copies the startup configuration into a file with a default name (***startup-config***), created in the script file system.

This command requires the startup configuration to be stored on the switch.

Command Syntax

```
device-name(config script-file-system)#copy-from startup-config [DEST-FILE]
```

Argument Description

DEST-FILE	(Optional) The name of the destination file, in the script file system.

Example

```
device-name(config script-file-system)#copy-from startup-config
saving script file "startup_config" to file system...  done
```

delete

The **delete** command, in Script-file-system Configuration mode, deletes the specified file from the file system.

NOTE  The specified file is deleted without requesting your confirmation.

Command Syntax

```
device-name(config script-file-system)#delete FILE-NAME
```

Argument Description

FILE-NAME	The name of the file to be deleted, in the script file system.

Example

```
device-name(config script-file-system)#delete test1
```

dir

The **dir** command, in Script-file-system Configuration mode, displays the names and lengths of all script files stored in the file system.

This command is equivalent to the **show script-file-system** command, but is available only in script file system configuration mode.

Command Syntax

```
device-name(config script-file-system)#dir
```

Example

```
device-name(config script-file-system)#dir
=====================================================
  no   |              name                 |    size
-------+-----------------------------------+----------
    1  | run_cnf1                          |       861
    2  | run_cnf2                          |       861
    3  | test1                             |       187
=====================================================
```

display

The **display** command, in Script-file-system Configuration mode**,** displays the textual contents of the specified script file.

Command Syntax

```
device-name(config script-file-system)#display FILE-NAME
```

Argument Description

FILE-NAME	The name of the script file, in the script file system.

Example

```
device-name(config script-file-system)#display test1
============= start file ==============
password a1h8rrzg11d4u
log trap errors
no banner
ip address 10.4.0.10 255.255.0.0
mac-address-table aging-time 300
============= end file ==============
```

download-from

The **download-from** command, in Script-file-system Configuration mode, copies the specified file from the TFTP server with the specified IP address to the file system on the switch. If an optional destination name is specified, the file is stored in the file system with this name. Otherwise, the file is stored with the source name.

Command Syntax

```
device-name(config script-file-system)#download-from A.B.C.D SOURCE-FILE
[DEST-FILE]
```

Argument Description

A.B.C.D	The IP address of the TFTP server.
SOURCE-FILE	The name of the source file that is copied from the TFTP server.
DEST-FILE	(Optional) The name of the destination file, in the script file system. If the name is not specified, the file is stored with the SOURCE-FILE name.

Example

```
device-name(config script-file-system)#download-from 10.4.0.4 test1.txt
test1
tftp receiving configuration ... 185
saving script to file system...
%% download complete
```

format file-system

The **format file-system** command, in Script-file-system Configuration mode, initializes the script file system for the first time. If the file system is already initialized, all the files that are stored in it are removed.

Before execution, a warning is issued requesting your confirmation to format the script file system.

Command Syntax

```
device-name(config script-file-system)#format file-system
```

Example

```
device-name(config script-file-system)#format file-system
all stored files will be removed. format? [y/n] : y
script file system formatted successfully
```

rename

The **rename** command, in Script-file-system Configuration mode, renames the specified script file.

Command Syntax

```
device-name(config script-file-system)#rename OLD-NAME NEW-NAME
```

Argument Description

OLD-NAME	The existing file-name in the script file system.
NEW-NAME	The name that replaces the existing file-name in the script file system.

Example

```
device-name(config script-file-system)#rename test1 test1.scr
file renamed
```

run

The **run** command, in Script-file-system Configuration mode, executes the CLI commands contained in the specified script file (as a batch file).

Before execution, a warning is issued requesting your confirmation to execute the batch configuration commands.

Command Syntax

```
device-name(config script-file-system)#run FILE-NAME
```

Argument Description

FILE-NAME	The name of the script file, in the script file system.

Example

```
device-name(config script-file-system)#run test1
batch configuration may interfere with a current one. execute? [y/n] : y
configuration from file successful
```

show script-file-system

The **show script-file-system** command, in Privileged or Script-file-system Configuration mode, displays the names and lengths of all script files stored in the file system.

This command is equivalent to the **dir** command, but may be used in View and Privileged modes.

Command Syntax

```
device-name(config script-file-system)#dir
```

Example

```
device-name#show script-file-system
=================================================
  no  |              name                |   size
------+----------------------------------+-------
    1 | run_cnf1                         |      861
    2 | run_cnf2                         |      861
    3 | test1                            |      187
=================================================
```

upload-to

The **upload-to** command, in Script-file-system Configuration mode, copies the specified file from the file system to a TFTP server with the specified IP address. If an optional destination name is specified, the file is stored on the server with this name. Otherwise, the file is stored with the source name.

Command Syntax

```
device-name(config script-file-system)#upload-to A.B.C.D SOURCE-FILE [DEST-FILE]
```

Argument Description

A.B.C.D	The IP address of the TFTP server.
SOURCE-FILE	The name of the source file that is copied from the script file system.
DEST-FILE	(Optional) The name of the destination file, in the TFTP server. If the name is not specified, the file is stored with the SOURCE-FILE name.

Example

```
device-name(config script-file-system)#upload-to 10.4.0.4 test1
%upload complete
```

scp

The **scp** command, in Script-file-system Configuration mode, allows for secure copying of files over insecure network.

Command Syntax

```
device-name(config script-file-system)#scp A.B.C.D NAME FILE [DEST-FILE]
```

Argument Description

A.B.C.D	The IP address of the TFTP server.
NAME	Username to use.
SOURCE-FILE	Name of the source file that is copied from the script file system.
DEST-FILE	(Optional). The name of the destination file, in the TFTP server. If the name is not specified, the file is stored with the SOURCE-FILE name.

Example

```
device-name(config script-file-system)#upload-to 10.4.0.4 test1
%upload complete
```

25. Status Monitoring, Statistics and General Commands

Overview

The commands described in this chapter are grouped in sections as summarized in Table 25-1.

Table 25-1 Status Monitoring, Statistics and General Commands

Section	Commands
System Information	show version
	show cpu utilization
	show system
Passwords	password
	enable password
Banner, Hostname and Service Commands	banner motd default
	banner set
	no banner
	hostname
	service advanced-vty
	service terminal-length
System Time and Date	date
	show date
	show clock
	time-server
Logging	log cli-console
	log telnet-console
	log trap
	log remote
Debug Information	debug stp
	debug rstp
	debug mstp
	debug mstp flush
	show debug

RMON	show rmon statistics
	snmp-server trap-community (see the Configuring and Displaying the SNMP Server Settings section)
	rmon event
	show rmon event
	rmon alarm counter
	show rmon alarm

Description of Commands

System Information

show version

The **show version** command, in View or Privileged (Enable) mode, displays the inventory information regarding the software and hardware versions of the switch.

Command Syntax

```
device-name#show version
```

Example

```
device-name#show version

N O K I A

Switch model   : NOKIA ESB26
SW version     : 3.3.0 created Jan 14 2004 - 15:59:00
Java version   : Java image not loaded
Loader version : 2.4 created Jan 30 2003 - 09:51:45

Up time        : 0 days, 1 hours, 21 min, 40 sec.
```

The asterisk (*) indicates that this is the current working version.

- **run to register** - indicates that the application in this bank exists and must be run to register itself in the **show version** command.
- **up time** displays the time elapsed since the unit was switched on.

show cpu utilization

The **show cpu utilization** command, in Privileged (Enable) mode, displays the CPU usage real time from switch startup.

ESB26 employs the lowest priority task scheduling mechanism to measure CPU utilization. This technique works by queuing a task that is supposed to run at the lowest possible priority in the system. This task is designed to be always ready to run. Since all useful application tasks have a priority higher than this task, the operating system will schedule this task only when it finds that no other task is in active state. Thus, the time this lowest-priority task is in active state actually represents the CPU idle time. The idle ticks provided by the task are counted by another process (which has the highest priority) and averaged for preset calculation periods.

The calculation of the CPU utilization is obtained by dividing the number of the idle ticks by the total ticks for a calculation period and presenting the result in percentage format indicating the CPU utilization (0-100%).

Command Syntax

```
device-name#show cpu utilization
```

Example

```
device-name#show cpu utilization
CPU usage 6%
```

show system

Displays system information for testing and debugging purposes. This command is intended only for Nokia technical support and is protected with a system password.

Passwords

Two password levels can be configured in the Nokia ESB26 switch.

- **View mode** password.
- Privileged mode password.

All passwords are encrypted. If you encounter problems in gaining access using the passwords, please contact Nokia support.

password

The **password** command, in Global Configuration mode, sets the switch's login password. The factory-default password is ***nokia***.

To enter View mode, when the switch is logged off, enter the password at the **password** prompt.

Command Syntax

```
device-name(config)#password PASSWORD PASS_CONFIRM
```

Argument Description

PASSWORD	A character string without blank spaces.
PASS_CONFIRM	Confirm password string

Example

```
device-name(config)#password switch123 switch123
```

enable password

The **enable password** command, in Global Configuration mode, sets a password to access Privileged mode from View mode. The **no** form of this command resets the default state. By default, no password is required to access Privileged mode.

When a password is set by the **enable password** command, a prompt for the password is issued in response to the **enable** command in View mode.

Command Syntax

```
device-name(config)#enable password PASSWORD PASS_CONFIRM
device-name(config)#no enable password
```

Argument Description

PASSWORD	A character string without blank spaces.
PASS_CONFIRM	Confirm password string

Example

```
device-name(config)#enable password switch123enable switch123enable
...
device-name>enable
Password: switch123enable
```

Banner, Hostname and Service Commands

NOTE  The banner commands will take effect only after reloading the switch.

banner motd default

The **banner motd default** command, in Global Configuration mode, sets the default motd (message-of-the-day) string. This is the ***hello*** string that will be displayed before *User Access Verification* and the password prompt.

Command Syntax

```
device-name(config)#banner motd default
```

banner set

The **banner set** command, in Global Configuration mode, assigns the specified string to *motd* (message-of-the-day). This string will be displayed before *User Access Verification* and the password prompt.

Command Syntax

```
device-name(config)#banner set MOTD_STRING
```

Argument Description

MOTD_STRING	Any string, including blank spaces and practically any character except for a question mark (?).

no banner

The **no banner** command, in Global Configuration mode, removes the *motd* (message-of-the-day) string set by the **banner motd default** or **banner set** command.

Command Syntax

```
device-name(config)#no banner
```

hostname

The **hostname** command, in Global Configuration mode, sets the name of the switch. This name appears in the beginning of each prompt-line. To remove the host name use the **no** form of this command.

Command Syntax

```
device-name(config)#hostname HOSTNAME
device-name(config)#no hostname
```

Argument Description

HOSTNAME	A character string starting with a letter followed by practically any characters except for blank spaces and question marks.

Example

```
default(config)#hostname switch_area1
```

```
switch_area1(config)#
```

service advanced-vty

The **service advanced-vty** command, in Global Configuration mode, enables advanced mode VTY. The **no** form of this command disables advanced mode VTY.

When advanced mode VTY is enables, the switch bypasses View mode at login and accesses Privileged mode directly. To access View mode, enter the **disable** command in Privileged mode.

Command Syntax

```
device-name(config)#service advanced-vty
device-name(config)#no service advanced-vty
```

service terminal-length

The **service terminal-length** command, in Global Configuration mode, determines the limit to the number of lines displayed on the terminal screen. The **no** form of this command resets the default value of 20 lines. A value of zero removes the limit.

This configuration command applies to all VTY interfaces.

Command Syntax

```
device-name(config)#service terminal-length <0-512>
device-name(config)#no service terminal-length
```

Argument Description

0-512	Limit to number of lines displayed on the screen. 0 represents unlimited length.

System Time and Date

This commands described in this section set the system time and date. You need to set the system time and date correctly for proper operation of key chains, and for keeping proper track of events in logging messages.

Table 25-2 Time and Date Commands

Command	Description
date	Sets the system time and date.
show date	Displays the current time and date.
show clock	Displays the current time and date, and optionally the synchronization client (if available).

time-server	Sets the switch to synchronize with the specified remote host.

date

The **date** command, in Global Configuration mode, sets the system time and date.

Command Syntax

```
device-name(config)#date HH:MM:SS <DAY> MONTH <YEAR>
```

Argument Description

HH:MM:SS	The current time (hours in 24-hour format, minutes and seconds).
DAY	Day of month in the range <1-31>.
MONTH	Name of month in English: *January, February*, *March*, *April*, *May*, *June*, *July*, *August*, *September*, *October*, *November*, *December*. (Capitalization is not required.)
YEAR	Year in four-digit number format in the 1993-2035 range.

Example

The following example sets system time to 12:30:00 and date 1 April 2004:

```
device-name(config)#date 12:30:00 1 apr 2004
```

show date

The **show date** command, in Privileged (Enable) mode, displays the current system time.

Command Syntax

```
device-name#show date
```

Example

```
device-name#show date
Current system time TUE APR 10 13:45:04 2001
```

show clock

The **show clock** command, in Privileged (Enable) mode, is an alternative form of the **show date** command, introduced for compatibility with other systems.

Command Syntax

```
device-name#show clock [detail]
```

Argument Description

detail	(Optional) If detail is specified, the command also displays the type of the currently used synchronization client. If detail is not specified, the command displays the current system time

Examples

1. The following example displays the date and time.

```
device-name(config)#show clock
Current system time TUE APR 10 13:45:04 2004
```

2. The following example displays the date and time, and also shows the currently used synchronization client (if available).

```
device-name(config)#show clock detail
Current system time TUE APR 10 13:45:04 2004
Time client is not used
```

3. The following example displays the date and time, and also shows the currently used synchronization client (if available):

```
device-name#show clock detail
Current system time THU JAN 01 00:01:02 1993

Time client is running with following peers:
Time server: 192.168.0.4
Refresh time: 10 minutes
Time zone shift: 2 hour(s)
```

time-server

The **time-server** command, in Global Configuration mode, sets your device to synchronize the system-time with the specified remote host. The no form of this command removes the timeserver definitions.

Remote system-time synchronization allows the system to accurately keep the correct time and date.

1. To use this feature, first choose the remote time synchronization protocol: "*Daytime protoco*l" (RFC867), "*Time protocol*" (RFC868)", or NTP (Network Time Protocol).

    - The "*Daytime Protocol*" specifies the date and time as a character string.
    - The "*Time Protocol*" specifies the time in seconds since midnight, January 1, 1900.
    - NTP, a highly accurate time synchronization protocol, has become a standard for Internet time synchronization. It requires additional configuration commands (including optional MD5 authentication). For details about NTP, refer to "NTP Client Description".

2. Configure the chosen time host service protocol;
3. Set the device for remote time synchronization.

The Server for remote synchronization may be any host running Windows NT/2000 or the UNIX operating system. To configure the Daytime or Timeserver, refer to your system documentation.

The **no** form of this command removes the timeserver definitions.

You can also synchronize the switch to observe the local daylight saving time in your area. For details, refer to "Configuring Daylight Saving Time (DST)".

Command Syntax

```
device-name(config)#time-server {time|daytime} A.B.C.D <refresh-time> [ZONE]
device-name(config)#no time-server

device-name(config)#time-server summer-time recurring (first1|<N1>|last1)
DAY1 MONTH1 HH:MM:SS1 (first2|<N2>|last2) DAY2 MONTH2 HH:MM:SS2 <T>

device-name(config)#time-server summer-time date <d1> MONTH1 <yyyy1> HH:MM:SS1
<d2> MONTH2 <yyyy2> HH:MM:SS2 <T>

device-name(config)#time-server daytime swap
```

NOTE

The old style of this command, wherein the IP address argument (A.B.C.D) precedes the time|daytime is supported for backward compatibility. However, Nokia strongly recommends using only the new style of the command for setting up time synchronization clients.

For details on **time-server summer-time** command, refer to "Configuring Daylight Saving Time (DST)".

Argument Description

time	Specifies "Time Protocol" (RFC868)
daytime	Specifies "Daytime Protocol" (RFC867)
swap	Swaps day and month (for daytime format). This would be required if the positions of day and month are interchanged in the daytimeserver's format, to prevent the switch from interpreting the day value as the month and the month value as the day.
A.B.C.D	IP address of the timeserver
refresh-time	Synchronization polling interval, in the range of <10-44640> minutes.
timeout *<timeout>*	Sets the timeserver session timeout in seconds. The range is <2-20> seconds.
ZONE	Shift of local hour relative to the server (Positive East, negative West of server's time zone).

Examples

1. The following command synchronizes the system time with host 192.168.0.1, using the Time Protocol. Synchronization will be performed every 10 minutes. Local time is two hours behind the server's time.

```
device-name(config)#time-server time 192.168.0.1 10 -2
```

2. The following command synchronizes the system time with host 192.168.0.1, using the

Daytime Protocol. Synchronization will be performed every 10 minutes. Local time is two hours ahead of the server's time.

```
device-name(config)#time-server daytime 192.168.0.1 10 2
```

show time-server

The **show time-server** command, in Privileged (Enable) mode, displays the timeserver configuration.

Command Syntax

```
device-name#show time-server
```

Example

```
device-name#show time-server

 Current system time MON OCT 13 19:00:25 2003

Timeserver protocol : daytime
Remote server IP     : 10.2.127.160
Refresh              : 10 min
```

Managing the Session Log

The following commands enable you to keep a log of your session.

log cli-console

The **log cli-console** command, in Global Configuration mode, directs log output (messages issued by the system) to the CLI console - attached to COM port.

The **no** form of this command stops log output to the CLI console.

Command Syntax

```
device-name(config)#log cli-console
device-name(config)#no log cli-console
```

log telnet-console

The **log telnet-console** command, in Global Configuration mode, directs log output (messages issued by the system) to the telnet console - if the user is connected through telnet client.

The **no** form of this command stops log output to the telnet console.

Command Syntax

```
device-name(config)#log telnet-console
device-name(config)#no log telnet-console
```

log trap

The **log trap** command, in Global Configuration mode, limits log output to the specified priority level. The **no** form of this command permits all logging information.

The priority is inversely related to the specified level (0 represents highest priority, 7 represents lowest priority). When you specify a priority level, logging output of the specified level and all lower levels is enabled. The priority levels of the log message types are listed in Table 25-3.

Table 25-3 Log Message Priority Levels

Priority level	Log message types
0	Emergencies (Only emergency messages are logged)
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging (All messages are logged)

Command Syntax

```
device-name(config)#log trap [emergencies|alerts|critical|errors|
warnings|notifications|informational|debugging]

device-name(config)#no log trap
```

log remote

The **log remote** command, in Global Configuration mode, enables remote logging. The **no** form of this command disables remote logging.

In addition to maintaining an internal log, the switch supports remote logging by way of the UNIX syslog host facility. To enable remote logging, do the following:

- Configure the syslog host to accept and log messages.
- Apply the **log remote** command in global Configuration mode.

For more information about the syslog host facility, refer to your syslog application documentation

Command Syntax

```
device-name(config)#log remote A.B.C.D

device-name(config)#no log remote [A.B.C.D]
```

Argument Description

A.B.C.D	IP address of the syslog host.

Example

The following command enables remote logging to host 192.1.22.14.

```
device-name(config)#log remote 192.1.22.14
```

Web Server Commands

Table 25-4 summarizes the web server commands.

Table 25-4 Web Server Commands

Command	Description
web-server	Enables the web server (BiNOSView).
show web-server	Displays the web server status.

web-server

The **web-server** command, in Global Configuration mode, enables the use of the web server (BiNOSView). The **no** form of the command disables use of the web server. By default, the web server is enabled.

Command Syntax

```
device-name#web-server
device-name#no web-server
```

show web-server

The **show web-server** command, in Privileged (Enable) mode, displays the web server status.

Command Syntax

```
device-name#show web-server
```

Example

```
device-name#show web-server
web-server enable
```

Debug Information

The following debugging commands can be used by support personnel to monitor a session as it proceeds on the switch.

debug mstp

The **debug mstp** command, in Privileged (Enable) mode, displays the information related to port roles, handshaking protocol, pim, prt, tcm and MAC address flush debugging in the Multiple Spanning Tree Protocol (MSTP). Use the **no** form of this command to disable the display of MSTP ports information.

The MSTP debug commands will not be saved after reload.

Command Syntax

```
device-name#debug mstp {roles | handshake | pim | prt | tcm | flush}
{all | <instance-id>}
device-name#no debug mstp {roles | handshake | pim | prt | tcm |
flush} {all | <instance-id>}
device-name#debug mstp bpdu {rx|tx|sanity-check validation}
{all|UU/SS/PP}
device-name#no debug mstp bpdu {rx|tx|sanity-check|instance-
id|validation} {all|UU/SS/PP}
```

Argument Description

roles	Displays logs of the port roles.
handshake	Displays port handshaking logs.
pim	Displays logs of the port information state machine.
prt	Displays logs of the port role transition state machine.
tcm	Displays logs of the topology change state machine.
flush	Displays logs of the MAC address table flush debugging.
all	Displays logs for all instances
instance-iddebug mstp bpdu	The MST instance ID, the range is 0 to 15.Displays logs for thereceived and transmitted BPDUs. For a detailed description, refer to 'Debugging the MSTP BPDU'.

debug rstp

The **debug rstp** command, in Privileged (Enable) mode, displays the RSTP debug messages. The **no** form of the command disables the debug messages.

The RSTP debug commands will not be saved after reload.

To view the debug messages you also need to enable **log cli-console** (for more information, see Managing the Session Log).

Command Syntax

```
device-name#debug rstp {all|handshake|roles|flush}
device-name#no debug rstp {all|handshake|roles|flush}
```

Argument Description

all	Activates all RSTP debug options.
handshake	Activates Hand Shake protocol debugging (IEEE 802.1w).
roles	Activates roles (designated port, root port, etc.) selection debugging.
flush	Activates port table flushing (MAC addresses) debugging.

debug stp

The **debug stp** command, in Privileged (Enable) mode, displays the STP debug messages. The **no** form of the command disables the debug messages.

The STP debug commands will not be saved after reload.

To view the debug messages you also need to enable **log cli-console** (for more information, see Managing the Session Log).

Command Syntax

```
device-name#debug stp {all|flush|tc|tcn}
device-name#no debug stp {all|flush|tc|tcn}
```

Argument Description

all	Activates all STP debug options.
flush	Activates MAC address table flush debgging.
tc	Activates the debug when the switch receives or transmits BPDU with topology change.
tcn	Activates the debug when the switch receives TCN or transmits BPDU with topology change ACK.

show debug

The **show debug** command, in Privileged mode, displays the status of the debug actions that are currently activated in the switch. Debug commands, which are activated in the Privileged mode, can be used by support personnel to monitor a session as it proceeds on the switch.

Command Syntax

```
device-name#show debug [mstp|rstp|stp]
```

Argument Description

mstp	Multiple Spanning Tree Protocol debugging information.
rstp	Rapid Spanning Tree Protocol debugging information.
stp	Spanning Tree Protocol debugging information.

26. Remote Monitoring

Introduction

Remote Monitoring *(RMON)* is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. This section provides a brief overview of the RMON specification, focusing on RMON groups.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Feature Overview

Packets Definitions

Good Packets

Good packets are error-free packets that have a valid frame length. For example, on Ethernet, good packets are error-free packets that are between 64 and 1518 octets long. They follow the form defined in IEEE 802.3.

Bad Packets

Bad packets are packets that have proper framing and are therefore recognized as packets, but contain errors within the packet or have an invalid length. For example, on Ethernet, bad packets have a valid preamble and Start of Frame Delimiter (SFD), but have a bad Cyclic Redundancy Check (CRC) or are either shorter than 64 octets or longer than 1518 octets.

RMON Groups

The ESB26 switch supports the following four RMON groups:

- Statistics
- History
- Alarms
- Events

The Ethernet Statistics Group

The Ethernet Statistics group contains statistics of packets, bytes, broadcasts, multicasts, and errors, measured by the probe for each monitored Ethernet interface on the switch.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of the network.

The History Group

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group.

The group is useful for analyzing traffic patterns and trends on an Ethernet interface on the switch and for establishing baseline information indicating normal operating parameters.

The Alarms Group

The Alarms group periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. Both rising and falling thresholds are supported, and thresholds can be specified on the absolute or delta value of a variable. In addition, alarm thresholds can be set manually or automatically.

Alarms inform you of a network performance problem and can trigger automated action responses through the Events group.

The Events Group

The Events group controls the generation and notification of events from the switch. The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore the event, to log it, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log the event and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

Effective use of the Events group saves you time. Rather than having to watch real-time graphs for important occurrences, you can depend on the Events group for notification. Through the SNMP traps, events can trigger other actions, which provide a mechanism for an automated response to certain occurrences.

Supported Standards, MIBs and RFCs

Standards

No standards are supported by this feature.

MIBs

RFC 1757, *Remote Network Monitoring Management Information Base*

RFCs

RFC 1757, *Remote Network Monitoring Management Information Base*

There are two RMON groups that can be used from the CLI:

- Statistics Monitoring;
- RMON Alarms.

The commands for each of them are featured in details below.

Statistics Monitoring

show rmon statistics

The **show rmon statistics** command, in Privileged (Enable) mode, displays statistics regarding the specified port. If no port is specified, statistics regarding all available ports on the switch are displayed.

Command Syntax

```
device-name#show rmon statistics [UU/SS/PP]
```

Argument Description

UU/SS/PP	(Optional) The port to display.

Example

1. Displaying statistics for a specified port, in Privileged mode:

```
device-name#show rmon statistics 1/1/3
octets             2430596        jabbers                  0
collisions               0        pkts                 26357
broadcast              488        pkts <=64           271222
multicast                0        pkts 65-127         110050
crcalignerrors           5        pkts 128-255         63053
undersize                1        pkts 256-511         36452
oversize                 0        pkts 512-1023         1491
fragments               36        pkts 1024-1518        2507
dropevents               0
```

2. Displaying statistics for all ports, in Privileged (Enable) mode:

```
device-name#show rmon statistics
interface 1/1/1
octets             2422964        jabbers                  0
collisions               0        pkts                 26266
broadcast              487        pkts <=64           270559
multicast                0        pkts 65-127         109304
crcalignerrors           5        pkts 128-255         62673
undersize                1        pkts 256-511         36316
oversize                 0        pkts 512-1023         1491
fragments               36        pkts 1024-1518        2507
dropevents               0

interface 1/1/2
```

```
octets                  9048        jabbers                 0
collisions                 0        pkts                   57
broadcast                  0        pkts <=64              39
multicast                  0        pkts 65-127            22
crcalignerrors             0        pkts 128-255           12
undersize                  0        pkts 256-511           10
oversize                   0        pkts 512-1023           0
fragments                  0        pkts 1024-1518          0
dropevents                 0

-- more --
```

RMON Alarms

Using CLI commands, the network administrator can define specific alarms indicating that some counters have passed the critical threshold. In this case, the switch sends trap that can be displayed in the network management platforms such as HP OV or SNMPc. To define these kinds of events, perform the following steps:

Step 1. Define the trap destination.

Step 2. Define event descriptions.

Step 3. Define alarm conditions.

Step 4. View RMON definitions in configuration list.

Defining and Viewing Event Descriptions

rmon event

The **rmon event** command, in Global Configuration mode, defines RMON event descriptions. The **no** form of this command removes the specified event. If no event-index is specified, all existing RMON events are removed.

Command Syntax

```
device-name(config)#rmon event <event-index> DESCRIPTION
{none|log|snmp-trap|trap-and-log} COMM OWNER

device-name(config)#no rmon event [<event-index>]
```

Argument Description

event-index	Event index in the range <1-65535>. If the index is new - event descriptions are created. If the index already exists - event descriptions are updated.
DESCRIPTION	Event description, without spaces.

none	No notification.
log	Log notification.
snmp-trap	SNMP-trap notification. (See the SNMP Server Configuration chapter)
trap-and-log	Log and trap notification.
COMM	Trap community (character string without blank spaces).
OWNER	Event owner (character string without blank spaces).

Examples

1. To define an RMON event description:

```
device-name(config)#rmon event 1 the_tank_is_full snmp-trap PUBLIC STN1
```

In this example:

- The event index is **1**;
- The event description is **the_tank_is_full**;
- The event notification is **snmp-trap**;
- The community string, as defined previously, is **PUBLIC**;
- The event owner is **STN1**.

2. To remove a particular event:

```
device-name#no rmon event 1
```

3. To remove all defined RMON events:

```
device-name(config)#no rmon event
remove all defined rmon events ? [y/n] : y
```

show rmon event

The **show rmon event** command, in Privileged (Enable) mode, displays the information for the specified RMON event. If no event index is specified, information on all currently defined RMON events is displayed.

Command Syntax

```
device-name#show rmon event [<event-index>]
```

Argument Description

event-index	(Optional) Event index in the range <1-65535>.

Examples

1. Displaying the currently defined RMON events:

```
device-name#show rmon event
event 1, status active, owned by stn1
```

```
description : the tank is full
type        : snmp-trap, lasttimesent: 01:36:29
community   : public
```

2. To display a particular RMON event:

```
device-name#show rmon event 1
```

Defining Alarm Conditions

rmon alarm counter

The **rmon alarm counter** command, in Global Configuration mode, defines RMON alarm conditions. The **no rmon alarm** command with a specified index removes the specified RMON alarm definitions. Without a specified index, **no rmon alarm** removes all defined RMON alarms.

Command Syntax

```
device-name(config)#rmon alarm <alarm-index> counter <1-17> UU/SS/PP
<1-4294967295> {absolute|delta} <rising-threshold>  <falling-threshold>
<rising-index>  <falling-index> OWNER

device-name(config)#no rmon alarm [<alarm-index>]
```

Argument Description

alarm-index	Alarm index, in the range <1-65535>. If the index is new - alarm conditions are created. If the index already exists - alarm conditions are updated.
1-17	Counter number, indicating one of the following: 1 DropEvents 2 Octets 3 Pkts 4 BroadcastPkts 5 MulticastPkts 6 CRCAlignErrors 7 UndersizePkts 8 OversizePkts 9 Fragments 10 Jabbers 11 Collisions 12 Pkts64Octets 13 Pkts65to127Octets 14 Pkts128to255Octets 15 Pkts256to511Octets 16 Pkts512to1023Octets

	17 Pkts1024to1518Octets
UU/SS/PP	Interface unit/slot/port
1-4294967295	Polling interval, seconds
absolute	Use absolute threshold values. The trap will be sent only once when the rising threshold value is met.
delta	Use threshold value differences. The agent will send the trap whenever the delta between the last and the current value reaches the rising or falling value. In the case of delta you should define two events - one for the case when the rising value is met and one for the case when the falling value is met.
rising-threshold	Rising-threshold, in the range <0-4294967295>
falling-threshold	Falling-threshold, in the range <0-4294967295>. Insignificant if absolute is specified.
rising-index	Rising-event index, in the range <0- 65535>
falling-index	Falling-event index, in the range <0- 65535>
OWNER	Alarm owner – character string without blank spaces.

Example

In the following example, the threshold type is **absolute** so the falling event is insignificant. The index is given an arbitrary value of zero.

If the threshold type were **delta**, the index would be assigned the number of the event of the falling value.

```
device-name(config)#rmon alarm 1 counter 2 1/1/3 5 absolute 20000 0 1 0 STN1
```

In this example the threshold type is absolute so the falling event is insignificant and that is why the index is zero.

If the threshold type is delta the index should be the number of the event of the falling value;

To remove all defined RMON alarms:

```
device-name(config)#no rmon alarm
remove all defined rmon alarms ? [y/n] : y
```

To remove a specific RMON alarm:

```
device-name#show rmon alarm 1
```

show rmon alarm

The **show rmon alarm** command, in Privileged (Enable) mode, displays the specified RMON alarm. If no argument is specified, all currently defined RMON alarms are displayed.

Command Syntax

```
device-name#show rmon alarm [<alarm-index>]
```

Argument Description

alarm-index	(Optional) Alarm index, in the range <1-65535>.

Examples

1. Displaying a specified RMON alarm, in Privileged mode:

```
device-name#show rmon alarm 1
```

2. Displaying the currently defined RMON alarms, in Privileged mode:

```
device-name#show rmon alarm
alarm 1, status active, owned by STN1
 counter octets, interface 1/1/3
 sampling interval (h:m:s) 00:00:05, sampletype absolute
 current value       5986918    startup : rising
 risingthreshold       20000    fallingthreshold           0
 risingeventindex          1    fallingeventindex          0
```

27. Periodic Monitoring

Introduction

The ESB26 switch monitors its own periodic operation.

For more reliable day-to-day operation, periodic crucial switch functions can be monitored in the background, alerting the network administrator when monitored indicators vary from operating norms.

As a troubleshooting tool, periodic monitoring can be used to catch transient conditions as they occur, and to track irregular behaviors. Because the periodic monitoring facility can generate SNMP traps, it can be used to trigger other diagnostic data polling based on the switch's operational status.

Table 27-1 displays the operational indicators that are monitored for ESB26:

Table 27-1 Periodic Monitoring Operational Indicators

Indicator	Monitored As
Temperature	Measured value
Ports	Measured value
CPU usage	Measured value
RAM usage	Measured value
Power supply	Pass/Fail

Feature Overview

There are two types of monitored indicators:

- **Pass/Fail conditions:** Is the power supply working? The monitor function returns a simple Pass or Fail operational status for power

- **Measured values**: What is the temperature? How many packet errors are there? The monitor function returns actual measured values for the port and temperature indicators.

Temperature monitoring measures the temperature using the Fahrenheit or Celsius scale.

Port monitoring measures error packets as CRC, Runts and Overrun.

$$\frac{(Total\ \ packets\ received) - (Total\ \ good\ \ packets\ received)}{Total\ \ good\ \ packets\ received} \times 100\%$$

Alert Behavior

An alert is generated when the Power indicator reports a Failed condition

-or-

the Temperature or Port indicator diverges from a preset limit value.

Two kinds of alert action are available:

- **log** – the alert status is written to a CLI interface's history and error message log files
- **trap** – an SNMP trap is generated.

Any or all of these actions can be assigned to an alert status. Alert behavior can be configured globally for all monitored indicators, or individually for specific indicators.

How Alerts are Triggered

There are two types of monitored indicators:

- *Pass/Fail conditions*: Is the power supply working? The monitor function returns a simple Pass or Fail status for power. When alert notification is enabled, alerts are triggered when the status is Fail.
- *Measured values*: What is the temperature? How many packet errors are there? The monitor function returns actual measured values for temperature and port operation. The **limit** and **delta** commands in Monitoring Configuration mode are used to define alert notification triggers for these indicators.

Limit-based Alert Triggering

A reference value can be set for the temperature,CPU and RAM indicator by using the **limit** command in Monitoring Configuration mode. You can set the condition that alerts will be generated only on the instance that the measured value rises above this reference, or only when it drops below this reference, or when it crosses the reference in either direction. For example, if you set alerts to be triggered when the measured value crosses the limit of 5 in either direction:

- An alert is triggered when the last measurement was 4 and the latest measurement is 6.
- No new alerts are triggered as long as measurements remain above 5.
- An alert is triggered when the measured value falls back below 5.

When the limit command is used alone, alerts are triggered only when the measured value crosses the limit value. The **delta** command in Monitoring Configuration mode can be used to configure a range of alert triggers relative to the limit value.

The delta command configures a scale centered on the limit value. The value of the delta command's <*difference*> variable determines *delta points*, which are points located along the scale on both sides of the limit value at distances that are whole multiples of <*difference*>:

… | <*difference*> | <*difference*> **limit** <*difference*> | <*difference*> | …

or:

..., [limit – 2 x (difference)] , [limit - difference] ,

[limit] ,

[limit + difference] , [limit + 2 x (difference)], ...

Alerts are triggered when the measured value crosses a unit-step of the scale. For example, if the limit is 55 and <*difference*> is 3, alerts may be generated when the value crosses any of these values:

…46, 49, 52, **55**, 58, 61, 64…

The trigger values differ from the limit value 55 by whole multiples of the <*difference*> value, in this case 3.

For *temperature* monitoring, the limit value is interpreted as degrees Fahrenheit or Celsius, depending on the scale selected for monitoring.

For *port monitoring*, the limit value is interpreted as the percent of error packets. This is defined differently for Full Duplex and Half Duplex traffic. For Full Duplex traffic, the error rate is calculated as:

Errors(Full-Duplex) = (Total_Pkts_In) - (MultiCast_Pkts_In + Unicast_Pkts_In)

For Half Duplex traffic, the error rate is calculated as:

Errors(Half-Duplex) = (Total_Pkts_In) - (MultiCast_Pkts_In + Unicast_Pkts_In + CRC_Align_Errs + Undersize_Pkts + Oversize_Pkts + Fragments)

Supported Standards, MIBs and RFCs

Standards

No standards are supported by this feature.

MIBs

No MIBs are supported by this feature.

RFCs

No RFCs are supported by this feature.

Default Periodic Monitoring Configuration

Table 27-2 shows the periodic monitoring default parameter values.

Table 27-2 Periodic Monitoring Default Parameter Values

Parameter	Default Value
Temperature monitoring	Enabled
Temperature monitoring scale	Celsius
Ports monitoring	Enabled
Power supply monitoring	Enabled
CPU usage	Enabled
RAM (memory) usage	Enabled
Log message alert	Enabled
Trap alert	Enabled
Limit values for monitoring alert	See table 27-3
Delta value for monitoring alert	Disabled
Monitoring period	See table 27-4

Table 27-3 Limit Values for Monitoring Alert Default Parameter Values

Parameter	Default Value
Limit value for temperature monitoring alert	55°C / 131°F
Limit value for ports monitoring alert	1%
Limit value for CPU usage monitoring alert	80%

Limit value for RAM usage monitoring alert	1000Kbytes

Table 27-4 Monitoring Period Default Values

Parameter	Default Value
Monitoring period for ports	10 seconds
Monitoring period for power supply	60 seconds
Monitoring period for temperature	20 seconds
Monitoring period for CPU usage	10 seconds
Monitoring period for RAM usage	30 seconds

Configuring and Displaying Periodic Monitoring

Enabling and Configuring Periodic Monitoring

Table 27-5 lists use of the **monitor** command to enable periodic monitoring.

Table 27-5 Commands to Enable Periodic Monitoring

Command	Description
monitor all	Enables or disables monitoring of all the periodic indicators.
monitor cpu-usage	Enables or disables monitoring of the CPU usage.
monitor ports	Enables or disables monitoring of the switch's ports.
monitor ram-usage	Enables or disables monitoring of the RAM usage.
monitor session	Enables or disables monitoring of the traffic.
monitor temperature	Enables or disables monitoring of the temperature.

Enabling/Disabling Periodic Monitoring Globally

The **monitor all** command, in Global Configuration mode, enables or disables the periodic monitoring of all periodic indicators. The **no** form of this command disables monitoring for all periodic indicators.

If no argument is specified, the command enables/disables all the alert options (***log*** and ***trap***).

If one of the arguments is specified, the command enables/disables only that alert option. By default, all the alert options are enabled.

By default, monitoring is enabled.

Command Syntax

```
device-name(config)#monitor all [log| trap] {enable|disable}
device-name(config)#no monitor all [log | trap]
```

Argument Description

log	Write alert messages to the log history.
trap	Send SNMP traps.
enable	Enable periodical monitoring of all the parameters.
disable	Disable periodical monitoring of all the parameters.

Monitoring CPU Usage

The **monitor cpu-usage** command, in Global Configuration mode, enables or disables monitoring of the CPU usage. The **no** form of this command disables monitoring of the CPU usage.

The CPU usage monitor constantly collects samples of CPU usage and periodically calculates their average value from previous percentage estimates. If the calculated value exceeds a configured limit value, the monitor issues a log alert.

To see the CPU usage, use the **show cpu utilization** command in Privileged (Enable) mode.

By default, CPU usage monitoring is enabled.

Command Syntax

```
device-name(config)#monitor cpu-usage {enable | disable}
device-name(config)#no monitor cpu-usage

device-name(config)#monitor cpu-usage
device-name(config monitor cpu-usage)#
```

Argument Description

enable	Enables monitoring of CPU usage.
disable	Disables monitoring of CPU usage.

Monitoring the Ports

The **monitor ports** command, in Global Configuration mode, enables or disables monitoring of the ports. The **no** form of this command disables monitoring of the ports.

You can use the command without arguments to enter into Monitoring Configuration mode for setting the port monitoring parameters.

By default, port monitoring is enabled.

Command Syntax

```
device-name(config)#monitor ports {enable | disable}
device-name(config)#no monitor ports

device-name(config)#monitor ports
device-name(config monitor ports)#
```

Argument Description

enable	Enables monitoring of ports.
disable	Disables monitoring of ports.

Monitoring the RAM (Memory) Usage

The **monitor ram-usage** command, in Global Configuration mode, enables or disables monitoring of the RAM usage. The **no** form of this command disables monitoring of the RAM usage.

The RAM usage monitor periodically checks the remaining amount of RAM that is available for allocation. If this amount is less than a configured limit value, the monitor issues a log alert.

By default, RAM usage monitoring is disabled.

Command Syntax

```
device-name(config)#monitor ram-usage {enable | disable}
device-name(config)#no monitor ram-usage

device-name(config)#monitor ram-usage
```

Argument Description

enable	Enables monitoring of RAM usage.
disable	Disables monitoring of RAM usage.

Monitoring the Traffic

The **monitor session command**, in Global Configuration mode, starts or ends a traffic monitoring session. For a detailed description of this command, refer to the Traffic Monitoring chapter.

Monitoring the Temperature

The **monitor temperature** command, in Global Configuration mode, is used to enable or disable temperature monitoring and to set the temperature monitoring scale to Celsius or Fahrenheit. The **no** form of this command disables temperature monitoring.

You can use the command without arguments to enter into Monitoring Configuration mode for setting the temperature monitoring parameters.

By default, temperature monitoring is enabled and the monitoring scale is Celsius.

Command Syntax

```
device-name(config)#monitor temperature {enable|disable|celsius|fahrenheit}
device-name(config)#no monitor temperature
```

```
device-name(config)#monitor temperature
```

Argument Description

enable	Enables monitoring of the temperature.
disable	Disables monitoring of the temperature.
celsius	Sets the scale for temperature monitoring to Celsius.
fahrenheit	Sets the scale for temperature monitoring to Fahrenheit.

Example

```
device-name(config)#monitor temperature fahrenheit
device-name(config)#monitor temperature
device-name(config monitor temperature F)#
```

NOTE 
The prompt of the temperature monitoring configuration mode indicates the temperature monitoring scale setting – C for Celsius or F for Fahrenheit.

Configuring Individual Periodic Monitoring Indicators

Table 27-6 lists the commands used to configure specific periodic monitoring indicators. You must enter into the specific monitoring indicator's configuration mode to use these commands. To see how to enter into each indicator's configuration mode, see table 27-5.

Table 27-6 Periodic Monitoring Configuration Commands

Command	Description
enable	Enables the periodic monitoring for a specific indicator.
disable	Disables the periodic monitoring for a specific indicator.
default	Restores the indicator's monitoring configuration to its default settings.
period	Sets the polling interval for monitoring.
log	Sends log messages for alert conditions by using the Syslog server.
trap	Enables trap alert notification options for a single indicator.
limit	Sets a limit value to trigger alerts.
delta	Sets a delta value to trigger alert conditions.

Enabling Periodic Monitoring for a Specific Indicator

The **enable** command, in Monitoring Configuration mode, enables the periodic monitoring for a specific indicator.

For default values, see table 27-2.

Command Syntax

```
device-name(config monitor INDICATOR)#enable
```

Example

The following example enables port monitoring:

```
device-name(config)#monitor ports
device-name(config monitor ports)#enable
```

Disabling Periodic Monitoring for a Specific Indicator

The **disable** command, in Monitoring Configuration mode, disables the periodic monitoring for a specific indicator.

For default values, see table 27-2.

Command Syntax

```
device-name(config monitor INDICATOR)#disable
```

Example

This example disables port monitoring:

```
device-name(config)#monitor ports
device-name(config monitor ports)#disable
```

Restoring the Default Monitoring Configuration

The **default** command, in Monitoring Configuration mode, restores the indicator's monitoring configuration to default settings.

Command Syntax

```
device-name(config monitor INDICATOR)#default
```

Setting the Monitoring Time Period

The **period** command, in Monitoring Configuration mode, sets the time intervals at which the indicator is polled for its status. The **no** form of the command resets the period to its default value.

Table 27-4 lists the default monitoring period values.

Command Syntax

```
device-name(config monitor INDICATOR)#period {hour|minutes|seconds} <value>
device-name(config monitor INDICATOR)#no period
```

Argument Description

hour	Sets monitoring period in hour unit.
minutes	Sets monitoring period in minute unit.
seconds	Sets monitoring period in second unit.
value	The number of hours, minutes, or seconds between polling instances. Valid values are <1-24> hours or <1-1440> minutes or <1-86400> seconds.

Example 1

The following example causes the ports to be checked every 3 seconds:

```
device-name(config monitor port)#period seconds 3
device-name(config monitor port)#
```

Example 2

The following example resets the temperature monitoring period to the default 60 seconds:

```
device-name(config monitor temperature C)#no period
device-name(config monitor temperature C)#
```

Setting Log Alert Notifications for a Specific Indicator

The **log** command, in Monitoring Configuration mode, enables logging alert notifications for a specific indicator.

If log alert notification is enabled, an alert message is written to the log and history files when:

- the indicator's status is "Failed"

-or-

- the indicator's measured value exceeds its configured limit

-or-

- the indicator's measured value crosses a configured delta point.

By default, log messages are enabled.

Command Syntax

```
device-name(config monitor INDICATOR)#log {enable | disable}
```

Argument Description

enable	Enables the monitoring alerts.
disable	Disables the monitoring alerts.

Example

This example enables log reporting for power monitoring:

```
device-name(config monitor power)#log enable
```

Setting Trap Alert Notifications for a Specific Indicator

The **trap** command, in Monitoring Configuration mode, enables SNMP trap alert notification for a single indicator.

If trap alerts are enabled, an SNMP trap is issued when:

- the indicator's status is "Failed"

-or-

- the indicator's measured value exceeds its configured limit

-or-

- the indicator's measured value crosses a configured delta point.

By default, the trap alert is enabled.

Command Syntax

```
device-name(config monitor INDICATOR)#trap {enable | disable}
```

Argument Description

enable	Enables the monitoring alerts.
disable	Disables the monitoring alerts.

Setting the Limit for Triggering Alerts

The **limit** command, in Monitoring Configuration mode, defines the limit value that triggers alert notifications. The **no** form of the command restores the limit to the default value. Specifying a zero value removes the limit.

Note that this command is available only for the temperature and port indicators.

Table 27-3 lists the default limit values for triggering monitoring alerts.

Command Syntax

```
device-name(config monitor INDICATOR)#limit <value>
device-name(config monitor INDICATOR)#no limit
```

Argument Description

value	The value of the limit. A zero value (0) disables limit-based alerts, and erases the limit.

Example 1

The following example sets a reference value of 7 percent error packets:

```
device-name(config monitor cpu-usage)#limit 7
```

Example 2

The following example restores the cpu-usage monitoring limit to 80

```
device-name(config monitor cpu-usage)#no limit
```

Setting Multiple Limits for Triggering Alerts

The **delta** command, in Monitoring Configuration mode, sets the scale used to trigger alerts as a measured value changes. The **no** form of the command restores the delta to its default value.

The command determines *delta points*, which are points located along the scale on both sides of a limit value at distances that are whole multiples of a specified <*difference*> value.

Specifying a zero value disables the delta alerts.

NOTE Delta tracing not available for port monitoring.

Command Syntax

```
device-name(config monitor INDICATOR)#delta <difference> [always|greater|less]
device-name(config monitor INDICATOR)#no delta
```

Argument Description

difference	The amount of change that triggers an alert. For temperature monitoring, the unit is degrees Fahrenheit or Celsius. .
always	Triggers an alert when the measured value rises above or drops below any delta point (the limit, plus or minus a multiple of <difference>).
greater	Triggers an alert when the measured value rises above any delta point that exceeds the limit by a multiple of <difference>).
less	Triggers an alert when the measured value falls below any delta point that is smaller than the limit by a multiple of <difference>).

Example 1

The following example triggers an alert when the measured temperature *exceeds* the limit by 5º, 10º, 15º, etc, but not when it is lower than the limit temperature:

```
device-name(config monitor temperature)#delta 5 greater
```

Example 2

The following example triggers an alert when the measured temperature is *higher or lower* than the limit by 3%, 6%, 9%, etc:

```
device-name(config monitor temperature)#delta 3 always
```

Example 3

The following example stops delta-based temperature monitoring:

```
device-name(config monitor temperature)#no delta
```

Displaying the Periodic Monitoring Configuration

Table 27-7 lists the commands used to display the periodic monitoring configuration.

Table 27-7 Periodic Monitoring Display Commands

Command	Description
show monitor	Displays the current periodic monitoring settings of all enabled indicators.
show	Displays the current periodic monitoring settings of a specific indicator.
show temperature	Displays the current Celsius (Centigrade) and Fahrenheit temperature at the unit's CPU area.

Displaying the Monitor Settings

The **show monitor** command, in Privileged (Enable) mode, displays the current periodic monitoring settings of all enabled indicators.

Command Syntax

```
device-name#show monitor INDICATOR | brief
```

Argument Description

INDICATOR	(Optional) Restricts the display to the specified indicator, for the list of the indicator supported by your platform. See table 27-8.
brief	(Optional) Displays the monitoring periods for all indicators.

Table 27-8 Indicator Parameters

Indicator	Description
cpu-usage	Monitoring the CPU usage.
ports	Monitoring the ports.
ram-usage	Monitoring the RAM (memory) usage.
session	Monitoring the traffic.
temperature	Monitoring the temperature.

Example 1

Use the command without any options to display the monitoring status of all enabled indicators:

```
device-name#show monitor

On-board Power Test
Period              : 60 sec.
Log                 : Enabled

Temperature Test
Period              : 20 sec.
Traps               : Enabled
Log                 : Enabled
Temperature limit   : 55C

Port Statistics Test
Period              : 10 sec.
Traps               : Enabled
Limit value         : 1%

CPU Resources Test
Period              : 10 sec.
Traps               : Enabled
Log                 : Enabled
Limit value         : 80%

RAM Resources Test
Period              : 30 sec.
Traps               : Enabled
Log                 : Enabled
Limit value         : 1000Kb
device-name#
```

Example 2

Use the **brief** option to display a summary of enabled indicators:

```
device-name#show monitor brief
On-board Power Test  : Period 60 sec.
Temperature Test     : Period 20 sec.
Port Statistics Test : Period 10 sec.
CPU Resources Test   : Period 10 sec.
RAM Resources Test   : Period 30 sec.
device-name#

device-name#show monitor temperature

Period              : 20 sec.
Traps               : Enabled
Log                 : Enabled
Temperature limit   : 55C
device-name#
```

Displaying a Specific Indicator's Configuration

The **show** command, in Monitoring Configuration mode, displays the current monitoring configuration for a specific indicator.

You can also use the **show monitor** command in Privileged (Enable) mode.

Table 27-4 lists the default monitoring period values.

Command Syntax

```
device-name(config monitor INDICATOR)#show
```

Example

The following example shows the configuration settings for temperature monitoring:

```
device-name(config monitor temperature C)#show
Period              : 20 sec.
Traps               : Enabled
Log                 : Enabled
Temperature limit   : 55C
```

Displaying the Temperature

The **show temperature** command, in Privileged (Enable) mode, displays the current Celsius (Centigrade) and Fahrenheit temperature at the unit's CPU area.

If the temperature reaches its higher limit (55°C or 131°F default), the switch can send an SNMP trap to the trap destination.

Command Syntax

```
device-name#show temperature [high-limit]
```

Argument Description

high-limit	(Optional) Displays the highest allowed Celsius (Centigrade) and Fahrenheit temperature at the unit's CPU area.

Example 1

```
device-name#show temperature
```

```
cpu temperature = 34C (93F)
```

Example 2

```
device-name#show temperature high-limit
cpu temperature high limit = 55C (131F)
```

Configuration Examples

CPU Usage Monitoring

In the following example, CPU usage monitoring is enabled and configured with both **limit** and **delta** commands.

1. Enable CPU usage monitoring:

```
device-name(config)#monitor cpu-usage enable
```

2. Enter into the CPU usage monitoring configuration mode:

```
device-name(config)#monitor cpu-usage
```

3. Display CPU usage monitoring settings:

```
device-name(config cpu-usage)#show

Period              : 10 sec.
Traps               : Enabled
Log                 : Enabled
Limit value         : 80%
```

4. Set the limit for CPU usage monitoring alerts to 5%:

```
device-name(config monitor cpu-usage)#limit 5
```

5. Set the delta to trigger alerts for changes of 1% in the error rate:

```
device-name(config monitor cpu-usage)#delta 1 greater
device-name(config monitor cpu-usage)#end
```

6. Display CPU usage monitoring configuration:

```
device-name#show monitor cpu-usage

Period              : 10 sec.
Traps               : Enabled
Log                 : Enabled
Limit value         : 5%
Delta value         : 1%
Notify on delta if criteria greater than limit
```

7. To check CPU usage monitoring, the trap output can be routed to the console:

```
device-name#configure terminal
device-name(config)#log cli-console
device-name(config)#log-history nvram trap errors
```

Traps are displayed on the CLI console. Note that the CPU usage is checked at 10 second intervals, as specified with the **period** command:

```
tHiSwMonitr: 1970/01/01 00:54:43 alerts: CPU Usage BIST fail:
7(limit 5)
tHiSwMonitr: 1970/01/01 00:54:43 alerts: CPU usage delta: current 7
tHiSwMonitr: 1970/01/01 00:54:53 alerts: CPU Usage BIST OK: 5(max 7)
tHiSwMonitr: 1970/01/01 00:55:03 alerts: CPU Usage BIST fail:
6(limit 5)
tHiSwMonitr: 1970/01/01 00:55:03 alerts: CPU usage delta: current 6
tHiSwMonitr: 1970/01/01 00:55:23 alerts: CPU usage delta: current 7
tHiSwMonitr: 1970/01/01 00:55:33 alerts: CPU Usage BIST OK: 5(max 7)
```

RAM Usage Monitoring

In the following example, RAM usage monitoring is enabled and configured with **period**, **limit** and **delta** commands.

1. Enable RAM usage monitoring:

```
device-name(config)#monitor ram-usage enable
```

2. Enter into the RAM usage Monitoring Configuration mode:

```
device-name(config)#monitor ram-usage
```

3. Display RAM usage monitoring settings:

```
device-name(config monitor ram-usage)#show

Period              : 30 sec.
Traps               : Enabled
Log                 : Enabled
Limit value         : 1000Kb
```

4. Set the limit for RAM usage monitoring alerts to 10%:

```
device-name(config monitor ram-usage)#limit 10
```

5. Set the delta to trigger alerts for changes of 3% in the error rate:

```
device-name(config monitor ram-usage)#delta 3 less
```

6. Set the period of alerts to 5 seconds:

```
device-name(config monitor ram-usage)#period seconds 5
device-name(config monitor ram-usage)#end
```

7. Display RAM usage monitoring configuration:

```
device-name#show monitor ram-usage

Period              : 5 sec.
Traps               : Enabled
Log                 : Enabled
Limit value         : 10Kb
Delta value         : 3Kb
Notify on delta if criteria less than limit
```

8. To check RAM usage monitoring, the trap output can be routed to the console:

```
device-name#configure terminal
device-name(config)#log cli-console
device-name(config)#log-history nvram trap errors
```

Traps are displayed on the CLI console. Note that the RAM usage is checked at 5 second intervals, as specified with the **period** command:

```
tHiSwMonitr: 1970/01/01 00:14:08  alerts: RAM Usage BIST fail: 134477
Kb(limit 124474Kb)
```

Related Commands

Table 27-9 shows the periodic monitoring related commands.

Table 27-9 Periodic Monitoring Related Commands

Command	Description	Described in
show cpu utilization	Displays the CPU usage in real time.	***Status Monitoring, Statistics and General*** Commands

28. Logging System Trap Messages to the NVRAM

Introduction

The System stores trap messages on the NVRAM. You cannot switch this logging feature off, but you may configure it to set the minimal priority level of messages that will be stored in the NVRAM.

Configuring the Trap Level for Stored System Messages

Trap messages generated by the system are categorized into the following levels:

- Emergency (highest level);
- Alert;
- Critical;
- Error;
- Warning;
- Notice;
- Information;
- Debug (lowest level).

You can configure the System to store messages from the Error level up. Lower level trap messages are never stored.

By default, only Emergency-level messages are stored on the NVRAM. All lower-level trap messages are filtered out.

To change the level of the trap-message logging filter, use the **log-history nvram trap** command (See NVRAM System-Trap Logging Commands). The setting will take effect on the next startup.

Configuring the Message Format

The structure of the stored (and displayed) system message is based on the following format:

```
SOURCE-TASK: DATE TIME  [PRIORITY]: MESSAGE-TEXT
```

Where:

SOURCE-TASK	is the name of a system task that generated the message.
DATE and TIME	indicate when the message has been issued.
MESSAGE-TEXT	is the textual content of the message.
PRIORITY	is the literal message's priority level.

The first three fields are always included in the message.

The **PRIORITY** field and is optional. By default this field is not included in any message. To force inclusion of the PRIORITY field in trap messages, use the **log record-priority** command (See NVRAM System-Trap Logging Commands).

NVRAM System-Trap Logging Commands

Table 28-1 summarizes the commands for controlling the logging of system trap messages on the NVRAM.

Table 28-1 NVRAM Logging Commands

Command	Description
log-history nvram trap	Specifies the lowest trap-message level that will be stored on the NVRAM.
log record-priority	Causes displayed and logged trap messages to include the optional PRIORITY field.
clear log nvram	Removes all System trap messages from the NVRAM
show log-history nvram	Displays the contents of the stored system message history.

Description of Commands

log-history nvram trap

The **log-history nvram trap** command, in Global Configuration mode, determines the lowest trap-message level that will be stored on the NVRAM. All trap messages of the specified and higher levels will be stored. To remove the log history, use the **no** form of this command.

NOTE

The show log-history nvram status command determines the priority level that limits trap messages currently stored. However, it does not indicate the minimal priority level of previously stored messages that exist in the NVRAM.

Command Syntax

```
device-name(config)#log-history nvram trap
{alerts|critical|emergencies|errors}
device-name(config)#no log-history nvram trap
```

Argument Description

emergencies	Sets the message log filter to the highest priority level (zero).
alerts	Sets the message log filter to priority level one.
critical	Sets the message log filter to priority level two.
errors	Sets the message log filter to the lowest allowable level.

log record-priority

The **log record-priority** command, in Global Configuration mode, causes displayed and logged trap messages to include the optional **PRIORITY** field. The no form of this command causes displayed and logged trap messages to exclude the optional **PRIORITY** field. By default, the **PRIORITY** field is excluded.

Command Syntax

```
device-name(config)#log record-priority
device-name(config)#no log record-priority
```

clear log nvram

The **clear log nvram** command, in Privileged (Enable) mode, removes all System trap messages from the NVRAM. The history starts from scratch.

Command Syntax

```
device-name#clear log nvram
```

show log-history nvram

The **show log-history nvram** command, in Privileged (Enable) mode, displays the contents of the stored system message history.

You can select output of the first (oldest) specified number of messages, the last (latest) specified number of messages, the size of the stored history (number of records), or the current trap-level status for history recording.

If no arguments are specified, the entire history is displayed. You can stop the output by pressing <Ctrl+C>.

Command Syntax

```
device-name#show log-history nvram [{{first <first-record>} |{last <last-record>}|size|status}}]
```

Argument Description

first <first-record>	(Optional) Displays the specified number of stored trap messages, starting at the oldest existing record. The range is <1-65535>.
last <last-	(Optional) Displays the latest specified number of stored trap messages. The

record>	range is <1-65535>.
size	(Optional) Displays the number of records in the system-message history.
status	(Optional) Displays the current trap-level status for history recording.

Examples

1. Displaying the current contents of the stored system message history:

```
device-name#show log-history nvram
  tcliuart: 2002/01/01 07:02:07  errors: test error message
  tcli_0: 2002/01/01 07:02:43  errors: test error message
  tcli_0: 2002/01/01 07:03:00  errors: test error message
  tcliuart: 2002/01/01 07:04:09  errors: test error message
  tcliuart: 2002/01/01 07:04:20  errors: test error message
  tcli_0: 2002/01/01 07:04:52  errors: test error message
  tcli_0: 2002/01/01 07:05:13  errors: test error message
  ttftptask: 2002/01/01 07:45:05  errors: transfer timed out.
  ttftptask: 2002/01/01 07:45:07  errors: tftpget: error occurred while
transferring the file.
  ttftptask: 2002/01/01 07:56:23  errors: transfer timed out.
  ttftptask: 2002/01/01 07:56:23  errors: tftpget: error occurred while
transferring the file.
  tcliuart: 2002/01/01 08:08:11 : test emergency message
  tcliuart: 2002/01/01 08:10:17 : test emergency message
  tcliuart: 2002/01/01 08:10:22 : test alert message
  tcliuart: 2002/01/01 08:10:31 : test critical message
  tcliuart: 2002/01/01 08:10:40 : test error message
  tcliuart: 2002/01/01 08:01:00 : test emergency message
  tcliuart: 2002/01/01 08:01:06 : test alert message
  tcliuart: 2002/01/01 08:01:11 : test critical message
  tcliuart: 2002/01/01 08:01:17 : test error message
```

2. Displaying the current trap-level status for recording history.

```
device-name#show log-history status
  Trap level of log history is errors (priority 3)
```

29. NVRAM Configuration History

Introduction

Configuration-history is a CLI feature, giving the user ability to record ALL the commands that were entered from Configuration mode into the device and changed the configuration. All the commands are recorded into the NVRAM even if the device configuration is not saved (with write command).

By default, Configuration-history recording is inactive.

History Log Format and Generation

Every time the user exits global Configuration mode, the configuration-session history is generated and stored into NVRAM in the following format:

```
!
! time_stamp :: user_id :: device{console|telnet|ssh}
! configuration session number start
!
command 1
command 2
….
!
! configuration session number end
!
```

The history session is stored in script-like format, so that user can easily re-execute the commands later.

Configuring History Settings

Table 29-1 summarizes the NVRAM History configuration Commands.

Table 29-1 Command-History configuration Commands

Command	Description
record configuration-history nvram	enables recording the configured commands into the NVRAM
clear configuration-history nvram	clears the history of configuration commands

Description of Commands

record configuration-history nvram

The **record configuration-history nvram** command, in Global Configuration mode, enables recording the configuration commands into the NVRAM. The **no** form of this command disables the recording, but does not clear it.

If you enable configuration-history recording, you must exit configuration mode for the command to take effect. Actual recording of configuration commands (not **show** commands) starts the next time you re-enter global Configuration mode and continues as long as that mode or any mode under it is active. In subsequent configuration sessions, as long as configuration-history recording is enabled, configuration commands accumulate in NVRAM by session.

If you disable configuration-history recording, recording stops immediately (you need not exit configuration mode for the command to take effect).

Command Syntax

```
device-name(config)#record configuration-history nvram
device-name(config)#no record configuration-history nvram
```

clear configuration-history nvram

The **clear configuration-history nvram** command, in Global Configuration mode, removes all the recorded configuration commands from NVRAM.

Command Syntax

```
device-name(config)#clear configuration-history nvram
```

Displaying the Configuration History

Table 29-2 summarizes the commands that display configuration-history information.

Table 29-2 Commands for Viewing Configuration-History Information

Command	Description
show configuration-history	Displays all configuration commands stored in the NVRAM during the specified session.
show configuration-history all	Displays all configuration commands stored in the NVRAM during all recorded sessions.
show configuration-history size	Displays the number of sessions currently stored in the NVRAM.
show configuration-history status	Displays the current recording state of configuration history (enabled or disabled).

Description of Commands

show configuration-history

The **show configuration-history** command, in Privileged (Enable) mode, displays all configuration commands stored in the NVRAM during the specified session. If no session number is specified, the command displays all configuration commands stored in the NVRAM during the last session.

Command Syntax

```
device-name#show configuration-history [<session-number>]
```

Argument Description

session-number	(Optional) Number of session displayed.

Examples

1. The following example displays the last configuration-session (two sessions were recorded):

```
device-name#show configuration-history
  ! MON MAR 11 07:18:03 2002 :: vty :: console
  ! Configuration session 2 start
  configure terminal
  ip address 131.119.251.201/24
  exit
  ! Configuration session 2 end
```

2. The following example displays the specified configuration-session (session number 1):

```
device-name#show configuration-history 1
  ! THU MAR 07 18:40:17 2002 :: vty :: console
  ! configuration session 1 start
  configure terminal
  network 36.0.0.0/24 area 36.0.0.0
  area 36.0.0.0 stub
  area 36.0.0.0 default-cost 20
  ! Configuration session 1 end
```

show configuration-history all

The **show configuration-history all** command, in Privileged (Enable) mode, displays all configuration commands stored in the NVRAM during all recorded sessions.

Command Syntax

```
device-name#show configuration-history all
```

Example

The following example displays all recorded configuration-sessions:

```
device-name#show configuration-history all
  ! THU MAR 07 18:40:17 2002 :: vty :: console
  ! Configuration session 1 start
  configure terminal
  network 36.0.0.0/24 area 36.0.0.0
  area 36.0.0.0 stub
  area 36.0.0.0 default-cost 20
  ! configuration session 1 end
  ! MON MAR 11 07:18:03 2002 :: vty :: console
  ! Configuration session 2 start
  configure terminal
  ip address 131.119.251.201/24
  exit
  ! Configuration session 2 end
```

show configuration-history size

The **show configuration-history size** command, in Privileged (Enable) mode, displays the number of sessions currently stored in the NVRAM.

Command Syntax

```
device-name#show configuration-history size
```

Example

```
device-name#show configuration-history size
Configuration history consists of 4 sessions.
```

show configuration-history status

The **show configuration-history status** command, in Privileged (Enable) mode, displays the current recording state of configuration history (as set by the **record configuration-history** command).

Command Syntax

```
device-name#show configuration-history status
```

Example

```
device-name#show configuration-history status
Configuration history recording enabled
```

30. Configuring the Watchdog Features

Overview

The Watchdog is a set of system features for monitoring some tasks or processes on the switch that are either critical or their monitoring is very useful for the administration of the switch. Unlike the other monitoring features however, it also triggers some automated actions to correct the situation if a monitored event or process goes wrong adding thus a bit of artificial intelligence to your switch.

The Watchdog is managed in a special Service Configuration mode called "Software Watchdog Configuration mode" (or "Watchdog mode" for short) and represented with the (sw-watchdog)# prompt on the display. To access the Watchdog mode, use the **service sw-watchdog** command in Global Configuration mode.

The Watchdog integrates three features:

1. **Reset-Loop Detection**:
   Detects and stops a reset-loop.

2. **SNMP Request Failure Detection**:
   Detects when an SNMP request fails and resets the switch.

3. **Application Suspension Detection**:
   Detects suspended applications and issues log notifications.

Each of these features is covered in detail later in this chapter.

Accessing Watchdog Mode

The **service sw-watchdog** command in Global Configuration mode provides access to Watchdog mode and its configuration options.

Command Syntax

```
device-name(config)#service sw-watchdog
```

Example

Accessing the Watchdog feature from View mode:

```
device-name>enable
device-name#configure terminal
device-name(config)#service sw-watchdog
device-name(sw-watchdog)#
```

Configuring the Reset-Loop Detection Feature

When this feature is enabled, the Watchdog detects when a reset-loop occurs and logs a notification about it to the NVRAM. The switch is considered to be in a rest loop when it resets more than 3 times in a certain time period. This period is configurable and can be set to 30÷1500 seconds. If a reset loop is detected, the switch reverts to a state where all LAN ports except the one configured as maintenance port are kept in physically disabled state.

By default, the Reset-Loop Detection feature is disabled.

Enabling Reset-Loop Detection

The **add sw-watchdog system reset-loop** command, in Watchdog Configuration mode, enables the Reset-Loop Detection feature, sets the reset loop detection time period and specifies the interface to be used as maintenance port when reset loop is detected.

Command Syntax

```
device-name(sw-watchdog)#add sw-watchdog system reset-loop <TIME> port <UU/SS/PP>
```

Argument Description

<UU/SS/PP>	Represents the unit, slot and port numbers of the interface configured as maintenance port in case of reset loop, e.g. 1/1/1.
<TIME>	Time period in seconds within which if more than 3 resets occur, the switch will be considered to be in a reset loop. The valid range is between 30 and 1500.

Example

To configure the switch to close all LAN ports except 1/1/1 if more than 3 reset loops occur within a 30-second period and to configure port 1/1/1 as maintenance port:

```
device-name(sw-watchdog)#add sw-watchdog system reset-loop 30 port 1/1/1
device-name(sw-watchdog)#
```

Disabling Reset-Loop Detection

The **remove sw-watchdog system reset-loop** command, in Watchdog mode, disables the Reset-Loop Detection feature and prevents the system from being monitored for reset loops.

Command Syntax

```
device-name(sw-watchdog)#remove sw-watchdog system reset-loop
```

Example

```
device-name(sw-watchdog)#remove sw-watchdog system reset-loop
device-name(sw-watchdog)#
```

Configuring the SNMP Request Failure Detection Feature

The SNMP Request Failure Detection feature monitors the timing and validity of the SNMP requests. If no valid SNMP request has been received within a specified time period, the request is considered lost and the feature resets the switch. The rationale is that the missing or invalid SNMP request indicates lost management network link and resetting the switch provides management access to it anew. This feature is fully configurable: it can be enabled/disabled and the SNMP request time out - specified in the range 10÷300 seconds.

By default, this feature is disabled.

NOTE

The SNMP Request Failure Detection feature should be enabled ONLY IF the SNMP server is configured to send periodic requests. Otherwise, the Watchdog will be interpreting the lack of SNMP requests as SNMP request failures and will be resetting the switch repeatedly thus forming a reset loop.

Enabling SNMP Request Failure Detection

The **add sw-watchdog system snmp-request-reset** command, in Watchdog Configuration mode, enables the SNMP request failure detection, specifies the timeout period and resets the device in case of SNMP request failure.

Command Syntax

```
device-name(sw-watchdog)#add sw-watchdog system snmp-request-reset <TIME>
```

Argument Description

<TIME>	Timeout for the SNPM request in seconds. If no valid response is received within the <Time> period, the switch will reset. The valid range is between 10 and 300.

Example

To configure the switch to reset if no valid response is received 5 minutes (300 seconds) after sending an SNMP request:

```
device-name(sw-watchdog)#add sw-watchdog system snmp-request-reset 300
device-name(sw-watchdog)#
```

Disabling SNMP Request Failure Detection

The **remove sw-watchdog snmp-request-reset** command, in Watchdog mode, disables the SNMP Request Failure Detection feature and prevents the system from being monitored for SNMP request failures.

Command Syntax

```
device-name(sw-watchdog)#remove sw-watchdog system snmp-request-reset
```

Example

```
device-name(sw-watchdog)#remove sw-watchdog system snmp-request-reset
device-name(sw-watchdog)#
```

Configuring the Application Suspension Detection Feature

The Application Suspension Detection monitors the switch for suspended applications and issues log notifications whenever an application is suspended. Application suspension usually means that the execution of that particular application has gone wrong so keeping track of suspended applications enables you detect and correct the problem in time. The Application Suspension Detection feature can be enabled/disabled. You have also the option to specify the applications to monitor for suspension or, alternatively, monitor all running applications.

By default, this feature is disabled.

Enabling Detection

The **add sw-watchdog application suspension** command, in Watchdog mode, enables monitoring for suspended applications and logs notifications to the NVRAM upon detecting a suspended application.

Command Syntax

```
device-name(sw-watchdog)#add sw-watchdog application all|<APPLICATION>
suspension
```

Argument Description

all	Enables monitoring of all applications.
<APPLICATION>	Name of the application to be monitored, e.g. **tLacp**. Enables monitoring of individual applications.

Example

To configure monitoring of the tLacp application:

```
device-name(sw-watchdog)#add sw-watchdog application tLacp suspension
tLacp_Susp added to watchdog
device-name(sw-watchdog)#
```

Disabling Application Suspension Detection

The **remove sw-watchdog application suspension** command, in Watchdog Configuration mode, disables the Application Detection Suspension feature and prevents the system from being monitored for suspended applications. When the feature is disabled, no notifications for suspended applications are sent to the NVRAM log.

Command Syntax

```
device-name(sw-watchdog)#remove sw-watchdog application all|<APPLICATION>
suspension
```

Argument Description

all	Disables monitoring of all applications.
<APPLICATION>	Name of the application the monitoring of which is to be ceased, e.g. **tLacp**. Disables monitoring of individual applications.

Example

To disable monitoring of the tLacp application:

```
device-name(sw-watchdog)#remove sw-watchdog application tLacp suspension
tLacp_Susp removed from watchdog
device-name(sw-watchdog)#
```

Displaying the Watchdog Configuration

To display the current Watchdog configuration in Priviledged (Enable) mode, use the **show sw-watchdog** command.

Command Syntax

```
device-name#show sw-watchdog
```

Example

```
device-name#show sw-watchdog
Watch Dog Objects status
=========================================
| No  |       Object       |     STATUS   |
=========================================
|1    |          tLacp_Susp|        FAILED|
|2    |            all_Susp|        FAILED|
device-name#
```

31. NTP Client Description

Introduction

NTP (Network Time Protocol) is a protocol built on top of TCP/IP that assures accurate local timekeeping with reference to radio, atomic or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long periods. It is defined in STD 12, RFC 1119 (definition from The Free On-line Dictionary of Computing, http://wombat.doc.ic.ac.uk/).

BiNOS's NTP Client supports all features described in RFC-1059 (Version 1), RFC-1119 (Version 2) and RFC-1305 (Version 3), except for the DES and RSA authentication mechanism. Support of these RFCs means that the NTP Client can synchronize its local clock with NTP servers that support any of these documents. The maximal number of remote NTP servers is restricted to 5. (BiNOS also supports the "Daytime" and "Time" remote synchronization protocols defined in RFC867 and RFC868 respectively. These protocols synchronize with only one server -- see the description of the **time-server** command in "The NTP Timeserver Commands").

NTP has become a standard for Internet time synchronization. Most importantly, there are more than 100000 free NTP timeservers in the world. Using the NTP protocol, the Nokia ESB26 switch time can be synchronized by the network administrator almost anywhere in the world with a minimal effort. Because of its mode of operation (a complicated election algorithm and MD5 authentication) and the Nokia ESB26 switch capabilities, the NTP Client is immune to almost any kind of network attack. Furthermore, the NTP Client guarantees high precision time synchronization.

In brief, the NTP Client features are:

- Ability to synchronize with RFC-1059 (Version 1), RFC-1119 (Version 2) or RFC-1305(Version 3) compatible NTP Servers;
- MD5 authentication algorithm;
- Up to 5 remote NTP timeservers for polling.

NOTE

Because of some newly introduced features in the time synchronization of the Nokia ESB26 switch, commands for setting time synchronization differ slightly from commands in older versions of BiNOS. Measures have been taken to preserve compatibility with older versions. The new version supports old style commands in order to permit execution of previously saved configurations.

However, it is strongly recommended NOT to use old style commands in the new version.

The NTP Timeserver Commands

Table 31-1 summarizes the NTP timeserver commands.

Table 31-1 NTP Timeserver Commands

Command	Description
time-server ntp add	Adds a server to the NTP server list.
time-server ntp delete	Deletes a server from the NTP server list.
time-server ntp show	Displays existing NTP timeserver list.
time-server ntp key add	Add authentication key.
time-server ntp key delete	Deletes authentication key.
time-server ntp key show	Displays existing NTP keys.
time-server ntp start	Starts NTP timeserver polling.

Why Use NTP Protocol ?

NTP is the most reliable of all time synchronization protocols. The advantages of NTP are:

- high redundancy, achieved by a complicated mechanism of processing incoming data;
- authentication of incoming data;
- widespread distribution of free, highly accurate NTP timeservers around the world;
- highly accurate time synchronization.

Configuring and Displaying NTP Server Settings

To run NTP synchronization you must set some parameters before starting to poll servers (You can configure the client to poll up to five remote NTP timeservers, in contrast to the "Daytime" and "Time" remote synchronization protocols that synchronize with only one server -- see the description of the **time-server** command in The NTP Time-Server Commands).

NOTE

1. Please read the information in the **www.ntp.org** site carefully to achieve efficient results in tuning and running an NTP server. This is important in order to fully test the NTP client of the switches.
2. For an NTP server to operate properly and with stability, it will be necessary to configure a few IP addresses of some actively working NTP timeservers.
3. An updated list of public primary and secondary NTP servers is available as well on the **www.ntp.org** site.

An NTP client can use up to a maximum of five servers. This requires the system administrator to define the IP addresses of the desired NTP servers. The following commands are used for adding, deleting and displaying NTP servers.

Description of Commands

time-server ntp add

The **time-server ntp add** command, in Global Configuration mode, adds a server to the NTP server list.

Up to five NTP servers can be defined. The switch will try to connect the NTP servers sequentially, in the order that they were inserted via the CLI.

Command Syntax

```
device-name(config)#time-server ntp add A.B.C.D
```

Argument Description

A.B.C.D	IP address of NTP server providing clock synchronization.

Example

The following example adds the NTP server with IP address 186.102.20.11.

```
device-name(config)#time-server ntp add 186.102.20.11
```

time-server ntp delete

The **time-server ntp delete** command, in Global Configuration mode, deletes the specified server from the NTP server list.

Command Syntax

```
device-name(config)#time-server ntp delete A.B.C.D
```

Argument Description

A.B.C.D	IP address of NTP server to be deleted.

Example

The following example deletes the NTP server with IP address 186.102.20.11.

```
device-name(config)#time-server ntp delete 186.102.20.11
```

time-server ntp show

The **time-server ntp show** command, in Global Configuration mode, displays the IP addresses of the currently defined NTP servers.

Command Syntax

```
device-name(config)#time-server ntp show
```

Example

The following example displays the three existing NTP servers.

```
device-name(config)#time-server ntp show

Current NTP server(s):
186.102.20.11
182.21.2.31
128.11.24.6
```

MD5 Authentication

NTP supports MD5 authentication. When using MD5 for the first time, you must assign it a key, consisting of a key ID and a plain text key. Only one key can be defined.

The key ID is a number in the range <1-65535>. The plain text key is a string of 1 to 20 non-blank characters (some special characters, such as question marks, are not allowed). The key authentication is case-sensitive (it distinguishes between capital and small letters). Once the key has been defined, NTP will use it to authenticate incoming data for all defined servers, until the key is deleted.

Servers that don't use authentication or servers that use an incorrect NTP key for an associated NTP client will be ignored.

Description of Commands

time-server ntp key add

The **time-server ntp key add** command, in Global Configuration mode, defines the MD5 authentication key.

Time synchronization can be authenticated to ensure that the local switch obtains its time services only from known sources. This authentication key must be coordinated with the administrator of the NTP server and must be matched by the servers used by the switch to synchronize its time to the NTP server.

By default, network time synchronization is unauthenticated.

Command Syntax

```
device-name(config)#time-server ntp key add <KEY-ID> KEY
```

Argument Description

KEY-ID	A number in the range <1-65535>.

KEY	A string of 1 to 20 non-blank characters (some special characters, such as question marks, are not allowed). Case-sensitive.

Example

The following example adds an MD5 authentication key with key ID of 27 and plain-text key **qwerty**.

```
device-name(config)#time-server ntp key add 27 qwerty
```

time-server ntp key delete

The **time-server ntp key delete** command, in Global Configuration mode, deletes the existing MD5 authentication key.

Command Syntax

```
device-name(config)#time-server ntp key delete [<KEY-ID> KEY]
```

Argument Description

KEY-ID	A number in the range <1-65535>.
KEY	(Optional) A string of 1 to 20 non-blank characters (some special characters, such as question marks, are not allowed).

time-server ntp key show

The **time-server ntp key show** command, in Global Configuration mode, displays the existing MD5 authentication key ID and string.

Command Syntax

```
device-name(config)#time-server ntp key show
```

Example

The following example adds an MD5 authentication key with key ID of 27 and plain-text key **qwerty**.

```
device-name(config)#time-server ntp key show

Current ntp authentication key:
1 qwerty
```

Running the NTP Server

The following commands start and stop NTP-Server polling.

time-server ntp start

The **time-server ntp start** command, in Global Configuration mode, starts the NTP-server polling.

NOTE To end the NTP server polling use the **no time-server** command in Global Configuration mode.

Command Syntax

```
device-name(config)#time-server ntp start <polling-interval> ZONE
```

Argument Description

polling-interval	The synchronization refresh period in minutes, in the range <10-44640> (The upper limit is equivalent to 31 days).
ZONE	Shift of local hour relative to GMT (Positive East, negative West of Greenwich).

Examples

1. The following example:
    - Configures the NTP Client by adding an NTP server without an authentication mechanism;
    - Starts the NTP client with a 10-minute polling-interval, and time zone GMT + 3 hours.

```
device-name(config)#time-server ntp add 192.168.0.2
device-name(config)#time-server ntp start 10 3
```

2. The following example sets the NTP Client with MD5 authentication:

```
device-name(config)#time-server ntp add 192.168.0.2
device-name(config)#time-server ntp key add 1 pass
device-name(config)#time-server ntp start 10 3
```

Configuration Example

The following example demonstrates how the switch uses an NTP server.

1. Add the NTP server:

```
device-name(config)#time-server ntp add A.B.C.D
```

2. Add an MD5 authentication key with key ID of 27 and plain-text key ***qwerty***:

```
device-name(config)#time-server ntp key add 27 qwerty
```

3. Start the NTP server polling with refresh period of 10 minutes and time zone 2:

```
device-name(config)#time-server ntp start 10 2
```

Configuring Daylight Saving Time (DST)

You can configure your switch to observe the daylight saving time in your area. This way, whenever the system time is corrected using a timeserver, it will be automatically corrected with the local DST time offset. The option can be set in two ways: as either recurring or one-time option. Table 31-2 lists the commands that invoke the recurring or the nonrecurring option, respectively.

Table 31-2 Daylight Saving Time Commands

Command	Description
time-server summer-time recurring	Configures the switch to perform DST adjustment that recurs yearly.
time-server summer-time date	Configures the switch to perform one-time DST adjustment on specified dates.

Enabling the Daylight Saving Time Adjustment

The **time-server summer-time recurring** command, in Global Configuration mode, configures the switch to adjust system time to daylight saving time in a recurring fashion. You specify the start and end dates and times for the DST and this time adjustment will repeat every year.

The **no** form of the command removes the summer time definition.

By default, the summer time definition is disabled.

Command Syntax

```
device-name(config)#time-server summer-time recurring
(first1|<N1>|last1) DAY1 MONTH1 HH:MM:SS1 (first2|<N2>|last2) DAY2 MONTH2
HH:MM:SS2 <T>
```

Argument Description

first$_1$	Configures the first week of ***MONTH***$_1$ as the start week for the DST.
<N$_1$>	Configures the week with the specified number (first, second, third, or forth of ***MONTH***$_1$) as the start week for the DST. The valid entries are the numbers from 1 to 4.
last$_1$	Configures the last week of ***MONTH***$_1$ as the start week for the DST.
DAY$_1$	Configures the day of the **first**$_1$**|<N$_1$>|last**$_1$ week (Sun-Mon) as the start day for the DST.
MONTH$_1$	Configures the start month (Jan-Dec) for the DST.
HH:MM:SS$_1$	Configures the exact time on ***DAY***$_1$ when the DST should begin.
first$_2$	Configures the first week of ***MONTH***$_2$ as the end week for the DST.
<N$_2$>	Configures the week with the specified number (first, second, third, or forth of ***MONTH***$_2$) as the end week for the DST.
last$_2$	Configures the last week of ***MONTH***$_1$ as the end week for the DST.
DAY$_2$	Configures the day of the **first**$_2$**|< N$_2$>|last**$_2$ week (Sun-Mon) as the start day for the DST.
MONTH$_2$	Configures the end month (Jan-Dec) for the DST.
HH:MM:SS$_2$	Configures the exact time on ***DAY***$_2$ when the DST should end.
<T>	Time adjustment specified in minutes from 1 to 1440.

Example

This example shows how to advance the system time automatically 1 hour every year, starting on the second Monday of April at 01:00:00 this year and move the system time back on the second Tuesday of October at 01:00:00.

```
device-name(config)#time-server summer-time recurring 2 mon apr
01:00:00 2 tue oct 01:00:00 60
```

Enabling Nonrecurring DST change on a Specific Date

The **time-server summer-time date** command, in Global Configuration mode, configures the switch to adjust system time to DST and then back to standard time on pre-set dates.

By default, DST adjystment is not scheduled.

Command Syntax

```
device-name(config)#time-server summer-time date <d1> MONTH1 <yyyy1>
HH:MM:SS1 <d2> MONTH2 <yyyy2> HH:MM:SS2 <T>
```

Argument Description

<d$_1$>	Configures the day on ***MONTH***$_1$ with the specified number (1-31) as the start day for the DST.

MONTH$_1$	Configures the month (Jan-Dec) of year **yyyy**$_1$ as the start day for the DST.
<yyyy$_1$>	Configures the start year for the DST. The valid values are from 1993 to 2035.
HH:MM:SS$_1$	Configures the exact time of the **d**$_1$ day when the DST should begin.
<d$_2$>	Configures the day on ***MONTH***$_2$ with the specified number (1-31) as the end day for the DST.
MONTH$_2$	Configures the month (Jan-Dec) of year **yyyy**$_2$ as the end day for the DST.
<yyyy$_2$>	Configures the end year for the DST. The valid values are from 1993 to 2035.
HH:MM:SS$_2$	Configures the exact time of the **d**$_2$ day when the DST should end.
<T>	Time adjustment specified in minutes from 1 to 1440.

Example 1

This example demonstrates advancing the system time 1 hour on May 1st, 2004, at 02:00:00 and moving it back on December 3rd, 2004, at 02:00:00.

```
device-name(config)#time-server summer-time date 1 May 2004 02:00:00
3 Dec 2004 02:00:00 60
```

Disabling DST Adjustment

The **no time-server summer-time** command, in Global Configuration mode, cancels any pending DST adjustments (set with **time-server summer-time**) and, if on DST, reverts the system clock to standard time

Command Syntax

```
device-name(config)#no time-server summer-time
```

32. Remote Authentication Dial-In User Service (RADIUS)

Introduction

RADIUS (Remote Authentication Dial-In User Service) is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server (switch), which requests to authenticate its links, and a shared Authentication Server. The current BiNOS RADIUS client supports login-type authentication only.

RADIUS communication uses UDP (User Datagram Protocol) with an assigned port number of 1812.

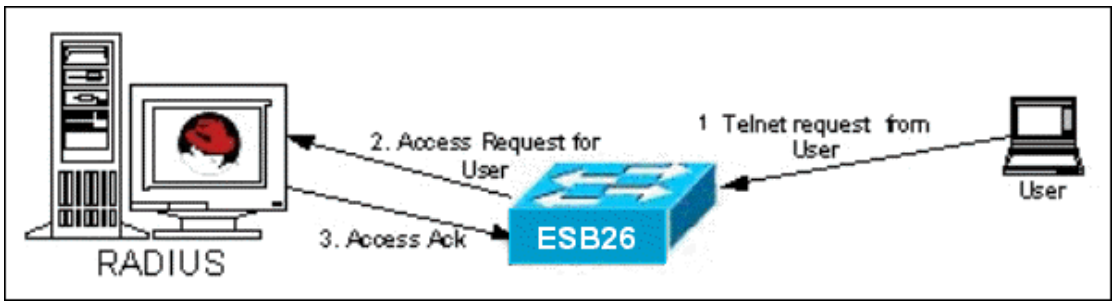


Figure 32-1 RADIUS Communication Example

Transactions between the switch and a RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords sent between the client and the RADIUS server are encrypted, to eliminate the possibility that anyone snooping on an insecure network could determine a user's password (the password is concealed by a method based on the RSA Message Digest Algorithm, MD5).

When the RADIUS server receives a request, it validates the sending client. If the RADIUS server does not have a shared secret with the client that sent the request, RADIUS will silently discard the request. Otherwise, the client is valid, and the RADIUS server consults a database of users to find the user whose name matches the request. The user entry in the database contains a list of requirements, which must be met to allow access for the user. This always includes verification of the password, but can also specify the client(s) or port(s) to which the user is allowed access.

BiNOS RADIUS Features

When a user attempts to log in and authenticate to an access server-using RADIUS, the following steps occur:

1. The user is prompted for and enters a username and a password.

2. The username and encrypted password are sent over the network to the RADIUS server.

3. The user receives one of the following responses from the RADIUS server:

- **ACCEPT**---The user is authenticated.
- **REJECT**---The user is not authenticated and is prompted to reenter the username and password, or access is denied.

The ACCEPT or REJECT packets also contain:

Reply message and user timeouts – session timeout and idle timeout.

Description of Commands

Commands to Configure a RADIUS Server Host

To specify a RADIUS server host and a shared password:

- Use the **radius-server host** command to define the remote RADIUS server host and optionally assign an authentication port number.
- Use the **radius-server key** command to specify the password shared with the remote RADIUS server host.

To customize communication between the switch and the RADIUS server:

- Use the **radius-server retransmit** command to specify how many times the switch transmits each RADIUS request to the server before giving up.
- Use the **radius-server timeout** command to specify how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
- Use the **radius-server deadtime** command to specify how many minutes a RADIUS server, which is not responding to authentication requests, is passed over by requests for RADIUS authentication.

radius-server host

The **radius-server host** command, in Global Configuration mode, defines the remote RADIUS server by specifying its IP address, and optionally assigns a UDP authentication port number. If the UDP authentication port number is not specified, the port number 1812 is assigned. The **no** form of this command deletes the specified host from the RADIUS database.

Command Syntax

```
device-name(config)#radius-server host A.B.C.D [<port-number>]
device-name(config)#no radius-server host A.B.C.D
```

Argument Description

A.B.C.D	The IP address of the RADIUS server.
port-number	Port number of the RADIUS server in range <1024-65535>

radius-server key

The **radius-server key** command, in Global Configuration mode, specifies the password used between the switch and the RADIUS server. The **no** form of this command removes the password.

Command Syntax

```
device-name(config)#radius-server key STRING
device-name(config)#no radius-server key
```

Argument Description

STRING	The shared secret text string used as a password between the switch and the RADIUS server.

radius-server retransmit

The **radius-server retransmit** command, in Global Configuration mode, specifies the number of times the switch transmits each RADIUS request to the server before giving up (default is three). The **no** form of this command restores the allowed number of retransmissions to the default value of 3.

Command Syntax

```
device-name(config)#radius-server retransmit <count>
device-name(config)#no radius-server retransmit
```

Argument Description

count	Number of allowed retransmissions, in the range <1-30>

radius-server timeout

The **radius-server timeout** command, in Global Configuration mode, specifies the number of seconds a switch waits for a reply to a RADIUS request before retransmitting the request. The default value is 3 seconds. The **no** form of this command restores the default value.

Command Syntax

```
device-name(config)#radius-server timeout <seconds>
device-name(config)#no radius-server timeout
```

Argument Description

seconds	Number of seconds between retransmissions, in the range <1-60>

radius-server deadtime

The **radius-server deadtime** command, in Global Configuration mode, specifies the number of minutes a RADIUS server, which is not responding to authentication requests, is passed

over by requests for RADIUS authentication. The **no** form of this command sets the dead-time to zero (non-responding servers are not passed over).

NOTE A configured RADIUS server is presumed dead, if timeout time is reached in three authentication sessions.

Command Syntax

```
device-name(config)#radius-server deadtime <minutes>
device-name(config)#no radius-server timeout
```

Argument Description

minutes	Dead-time interval in minutes, in the range <0-1440>

Creating the Local Database

The local authentication database is used for authentication if the configured radius server is not responding.

For details on how to use the **username** command, refer to "Creating a New User with a Privilege Level".

Using RADIUS to Configure Login Authentication

Use the **aaa authentication login default** command with the radius method keyword to specify RADIUS as the login authentication method.

aaa authentication login default

The **aaa authentication** command, in Global Configuration mode, specifies the default login authentication method. The **no** form of this command disables authentication – except for the login password.

Local authentication is tried only if there is no response from the RADIUS server.

NOTE The secondary authentication method is always local. This is to prevent the situation that you cannot configure authentication on an interface because RADIUS authentication prevents you from logging in.

Command Syntax

```
device-name(config)#aaa authentication login default PRIMARY SECONDARY
device-name(config)#no aaa authentication login default
```

Argument Description

PRIMARY	Primary authentication method, either radius or local.
SECONDARY	Secondary authentication method must be local.

A RADIUS Configuration Example

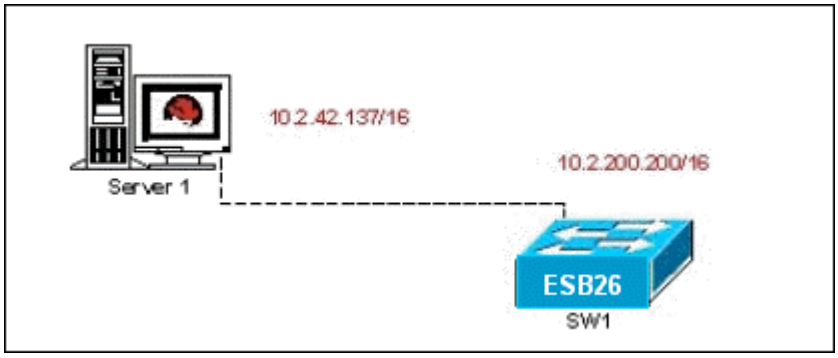


Figure 32-2 RADIUS Configuration Example

To demonstrate a RADIUS configuration, proceed as follows:

1. Install a RADIUS server on Server 1.
2. Configure the RADIUS server.
3. Edit RADIUS Server's Clients File and add the switch IP address with a distinctive key:
    - Add the line

```
10.2.200.200    123456
```

Edit the RADIUS Server's Users File:

- Add two users as follows:

```
johnwilliams   auth-type = local,  password = "h5yr9b"
               reply-message = "user is in"

jamessmith     auth-type = reject
               reply-message = "your payment balance is outstanding - access
               denied"
```

Configure the Switch:

- In the switch CLI configure the RADIUS Server host and key as follows:

```
device-name(config)#radius-server host 10.2.42.137
device-name(config)#radius-server key 123456
```

- Add local user with username of localUser and password MyPass:

```
device-name(config)#username localuser password mypass
```

NOTE Local authentication database is used for authentication if the configured RADIUS Server is not responding.

- Begin authentication option using the command:

```
device-name(config)#aaa authentication login default radius local
```

- Add retransmit, timeout and deadtime parameters as follows:

```
device-name(config)#radius-server retransmit 3
device-name(config)#radius-server timeout 10
device-name(config)#radius-server deadtime 3
```

Save the configuration and restart the switch

The results of the above configuration will be as shown in the examples below:

If you try to access the switch using Username “jamessmith”, the result will be REJECT:

```
username: jamessmith
password: your payment balance is outstanding - access denied
username:
```

If you try to access the switch using Username "johnwilliams" Password “h5yr9b”, the result will be ACCEPT

```
username: user
password: user is in
device-name#
```

If you try to access the switch using Username: “localUser” Password “MyPass, the result will be an Authentication Failure from the RADIUS Server.

If the RADIUS Server is shut down or disconnected from the switch and you try to access the switch with Username: “localUser” Password: “MyPass”, the result will be ACCEPT. After the last three queries, the switch will log in successfully using the local authentication database.

33. Secure Shell (SSH)

Introduction

SSH Secure Shell is the standard authentication protocol used for protecting data from malicious intruders through the Internet, prevention of password stealing, etc. SSH Version 2 supports multiple public key algorithms, including DSA (Digital Signature Algorithm).

The BiNOS SSH (Secure Shell) server, using SSH Version 2, provides you with a more secure connection to your Nokia ESB26. The BiNOS SSH server supplies user authentication service by a password authentication method. The BiNOS SSH server does not support SFTP, tunneling or any other method except for a remote secured login connection. The BiNOS SSH server supports only one channel per connection.

Some Security Considerations

When you log into the SSH server for the first time, the SSH client usually issues a security alert message such as:

Regard this as a warning that the security and secrecy of the data on your computer may be jeopardized. If in a later login the same message appears (even though you have confirmed your trust on the initial connection), then either you are exposed to a malicious intrusion, or the server administrator has reconfigured the keys.

The keys are configured with the **ssh generate-key dsa** command described below. When using an SSH client to log into a Nokia ESB26 device, avoid using a telnet client from that device to another host. This precaution is required to prevent making the secure connection vulnerable to anyone who may spy on both network connections.

To configure the user name and password, use the **username** command in Global Configuration mode.

Commands for Managing the SSH Server.

The SSH commands are summarized in Table 33-1. All commands for managing the SSH server are available in the switch's global Configuration mode.

Table 33-1 SSH Commands

Command	Description
ssh generate-key dsa	Generates the starting public parameters for the DSS algorithm that is used in the key-exchange phase of the login.
ssh start	Initializes and starts the BiNOS SSH server.
ssh stop	Stops the BiNOS SSH server.

Remember that before you can use SSH, you must enable some kind of a user database on the device. You can use the local database and locally create usernames and passwords, or use the BiNOS RADIUS client application.

Description of Commands

ssh generate-key dsa

The **generate-key dsa** command, in Global Configuration mode, generates the starting public parameters for the DSA algorithm that is used in the key-exchange phase of the login (For more information, see **Supported Standards** below). Remember that you must enter this command before starting your BiNOS SSH server for the first time.

Save the current configuration to avoid losing the parameters on reboot.

To change the parameters, use the same command. If at the moment of running the command the SSH server is started, you must apply the **ssh start** and **ssh stop** commands so the changes take effect.

Command Syntax

```
device-name(config)#ssh generate-key dsa
```

ssh start

The **ssh start** command, in Global Configuration mode, initializes and starts the BiNOS SSH server. You can log safely into the device only after running the **ssh start** command.

Command Syntax

```
device-name(config)#ssh start
```

ssh stop

The **ssh stop** command, in Global Configuration mode, stops the BiNOS SSH server. Keep in mind that by stopping the server, you close all current SSH connections to the device.

Command Syntax

```
device-name(config)#ssh stop
```

Supported Clients

You can use the BiNOS SSH server with SSH clients such as:

- The SSH client of SSH Communications Security Corp.
- The OpenSSH secure shell client.
- The PuTTY terminal program.
- The F-Secure SSH client
- Any other client that supports SSH (version 2)

Supported Standards

- draft-ietf-secsh-architecture-07
- draft-ietf-secsh-transport-09
- draft-ietf-secsh-connect-09
- draft-ietf-secsh-userauth-09
- FIPS 186 (Digital Signature Standard)
- FIPS 180-1 (Secure Hash Algorithm)
- RFC 1851 3DES-CBC and BLOWFISH-CBC cipher
- RFC 2792 DSA Key and Signature Encoding for the KeyNote Trust Management System
- HMAC-SHA1 MAC algorithm

34. 802.1X Port-Based Authentication

Introduction

The IEEE 802.1X standard offers a method for controlling port access in a central location on a user or device basis. 802.1X helps to facilitate the control of networks.

The 802.1X (or *dot1x*) standard relies on the supplicant (user or client that requests authentication) to provide credentials in order to gain access to the network. The credentials can be a username/password combination or a certificate. The credentials are not verified by the switch but are sent to a Remote Authentication Dial-In User Service (RADIUS) server, which maintains a database of authentication information.

Dot1x acts as Authenticators in a local network. BiNOS supports the MD5 authentication method without accounting.

Feature Overview

IEEE 802.1X standard relies on the Extensible Authentication Protocol (EAP) and passes it over a wired or wireless LAN. EAP is an authentication protocol that provides a framework for authentication methods instead of simply employing usernames and passwords for access.

The protocol in 802.1X is called EAP encapsulation over LANs (EAPOL). Communication between supplicants in the network and the Authentication Server is performed through EAPOL packets.

802.1X consists of three components for port control – Supplicant, Authentication Server and Authenticator.

Supplicant

A *supplicant* is the user or client that wants to be authenticated. This is the end device that connects to a switch and requests to use the services (port) of the device. The 802.1X supplicant must be able to respond to EAP packets.

Authentication Server

Authentication Server is the actual server that authenticates the supplicants and typically, this is a RADIUS server. The RADIUS server examines the credentials provided to the authenticator from the supplicant and provides the authentication service.

Authenticator

Authenticator is the device in-between the supplicant and the authentication server. The 802.1X key point is that the authenticator is very simple as the supplicant and the authentication server performs most of the authentication process.

Mode of Operation

When a BiNOS switch is configured as an authenticator, the ports of the switch must be configured for authorization.

When the authenticator detects that the link with the supplicant is active and an EAPOL start-packet is received, the authenticator port sends an EAP packet to the supplicant requesting the supplicant's identification. If the supplicant attached to the switch does not understand the EAP packet that is received from the switch, it does not send an ID and the port remains unauthorized. In this state, the port does not pass any user traffic. If the supplicant is running the 802.1X EAP, it responds to the request with its configured ID.

When the authenticator receives the ID from the supplicant, it passes the ID information to an authentication server (RADIUS server).

The authentication server sends back a challenge to the authenticator. The authenticator repackages it into EAPOL, and sends it to the supplicant.

The supplicant responds to the challenge via the authenticator and passes the response to the authentication server.

If the supplicant provides a proper ID, the authentication server responds with a success message, which is then passed onto the supplicant. If the response is a failure, the port remains unauthorized and no user traffic is allowed to pass through It. The port also remains unauthorized and does not pass any traffic, if there is no response from the RADIUS server. It is possible to configure the switch to use multiple radius servers in the event that the server is unreachable.

Figure 34-1 displays the process of authorization.

Figure 34-1 Authentication Process

The authenticator and the supplicant communicate with each other through Layer2 EAPOL packets, while the authenticator and RADIUS server communicate through IP/UDP RADIUS packets. The authenticator performs EAPOL ↔ IP/UDP RADIUS packets capsulation.

Supplicant Modes

802.1X supports three supplicant modes: *Single Host*, *Multiple Hosts* and *Multiple Hosts/Per MAC mode*. The table below shows the 802.1X supplicant modes.

Table 34-1 802.1X Supplicant Modes

Mode	Description
Single Host	Only one supplicant may be authorized on a port. If several supplicants request authorization, the first one that authenticates successfully is authorized, and all the others are rejected without trying to authenticate them. This is the default supplicant mode.
Multiple Hosts	More than one supplicant can be authorized on a port. The first one that authenticates successfully unlocks the port and the other supplicants have full access to the device services.
Multiple Hosts/Per MAC mode	More than one supplicant can be authorized on a port. Each supplicant is authenticated individually. You can set a maximum number of supplicants per port. When this limit is reached, new supplicants are rejected without trying to authenticate them. The default setting for this supplicant mode is no maximum limit.

NOTE 802.1X supplicant modes can be set per port.

Traffic Modes

802.1X supports two traffic modes: *Bi-directional traffic control* and *Unidirectional traffic control*. The table below shows the 802.1X traffic modes.

Table 34-2 802.1X Traffic Modes

Mode	Description
Bi-directional traffic control	Unauthorized supplicants on locked ports have neither incoming nor outgoing traffic. This is the default traffic mode.
Unidirectional traffic control	Unauthorized supplicants on locked ports have only incoming traffic. All outgoing traffic is rejected.

NOTE 802.1X traffic modes are set globally on the switch.

Ports in Authorized and Unauthorized States

The switch port state determines whether or not the supplicant is granted access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a supplicant is

successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the supplicant to flow normally.

If a supplicant that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the supplicant's identity. In this situation, the supplicant does not respond to the request, the port remains in the unauthorized state, and the supplicant is not granted access to the network.

In contrast, when an 802.1X-enabled supplicant connects to a port that is not running the 802.1X protocol, the supplicant initiates the authentication process by sending the EAPOL-start frame. When no response is received, the supplicant sends the request for a fixed number of times. Because no response is received, the supplicant begins sending frames as if the port is in the authorized state.

The port authorization state is controlled by specifying one of the following control types in the **dot1x port-control** command:

- **force-authorized** - disables 802.1X authentication and causes the port to transition to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based supplicant authentication. This is the default setting.
- **force-unauthorized** - causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The switch cannot provide authentication services to the supplicant through the interface.
- **auto** - enables 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. The switch uniquely identifies each supplicant attempting to access the network by the supplicant's MAC address.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a supplicant logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Supported Standards, MIBs and RFCs

Standards

IEEE 802.1X, Standard for Local and metropolitan area networks - Port-Based Network Access Control

MIBs

No MIBs are supported by this feature

RFCs

RFC 2856*, Remote Authentication Dial In User Service (RADIUS)*

RFC 2869, *Remote Authentication Dial In User Service (RADIUS) Extensions*

Default 802.1X Configuration

The table below shows the default 802.1X configuration.

Table 34-3 802.1X Default Configuration

Parameter	Default Value
Maximum number of requests	2
Re-authentication	Disabled
Re-authentication period	3600 seconds
Quiet timer period	60 seconds
Period for communication timeouts	30 seconds
Traffic Control Mode	Bi-directional
Authorization mode	Force-Authorized
Supplicant Mode	Single-Host mode
Debug 802.1X	Disabled

Configuring and Displaying 802.1X

The BiNOS 802.1X implementation consists of configuring the three participants for operation. Supplicants that connect to 802.1X authenticators are required to support EAP. The 802.1X implementation needs at least one RADIUS server to be configured. Dot1x works with every RADIUS server that is compatible with RFC 2865 and RFC 2869, as well as with every 802.1X supplicant that is compatible with the IEEE 802.1X standard. The RADIUS server and the supplicant must be configured with the proper authentication identification: passwords and usernames or certificates and certificate authorities. Third-party supplicants must also be configured to use the protocol for the adapters and with the appropriate ID information. This varies depending on the 802.1X supplicant software. The RADIUS server must be configured with the IP address of any device that requests information. It must also be configured with a unique key that must also be configured on the switch. Finally, the RADIUS server must be configured and the switch must be configured as authenticator. For more information regarding the RADIUS server, see "*Understanding and Configuring Remote Authentication Dial In User Service (RADIUS)*".

This setting enables the 802.1X port authentication process and makes the switch an authenticator. Configured as Authenticator, the switch is able to send the EAP messages to the supplicant, proxy the information to the configured authentication (RADIUS) server(s), and act on the messages received from those servers to authorize ports.

The authenticator ports can be in one of three authorization modes: **force-authorized** (the default mode), **auto** and **force-unauthorized**. To set the ports' mode, proceed according to the following guidelines:

1. Enter into Interface Configuration mode.

2. Set 802.1X to the particular control type for the specified port. See Setting the Control Type for a Specified Port.

802.1X Global Configuration Commands

The table below lists the 802.1X global configuration commands.

Table 34-4 802.1X Global Configuration Commands

Command	Description
dot1x max-req	Sets the number of times that the switch sends an EAP-request/ identity frame to the supplicant before restarting the authentication process.
dot1x re-authentication	Enables periodic re-authentication of the supplicant.
dot1x re-authenticate	Activates the process of re-authentication on all supplicants and for all ports.
dot1x timeout host	Sets the supplicants' authentication timeout period.

dot1x timeout re-authperiod	Sets the number of seconds between re-authentication attempts.
dot1x timeout quiet-period	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the supplicant.
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request.
dot1x unicast-client-compatibility	Sets a mode that allows dot1x to work with supplicants, but without sending EAPOL packets to 802.1X group MAC addresses.

Setting the Maximum Number of Requests to the Supplicant

The **dot1x max-req** command, in Global Configuration mode, sets the number of times that the switch sends an EAP-request/identity frame to the supplicant before restarting the authentication process. The **no** form of this command reset this value to its default.

By default, the maximum number of requests is 2.

Command Syntax

```
device-name(config)#dot1x max-req <requests-number>
device-name(config)#no dot1x max-req
```

Argument Description

requests-number	The maximum number of request is in range <1-10>.

Example

```
device-name(config)#dot1x max-req 3
```

Enabling Periodic Re-authentication

The **dot1x re-authentication** command, in Global Configuration mode, enables periodic re-authentication of the supplicant. The **no** form of this command disables the re-authentication.

You can enable periodic 802.1X supplicant re-authentication and specify how often it occurs. If you do not specify a time period, the number of seconds between re-authentication attempts is 3600. To set the time period, use the **dot1x timeout re-authperiod** command in Global Configuration mode.

By default, the re-authentication is disabled.

Command Syntax

```
device-name(config)#dot1x re-authentication
device-name(config)#no dot1x re-authentication
```

Example

```
device-name(config)#dot1x re-authentication
```

Forcing the Process of Re-authentication

The **dot1x re-authenticate** command, in Global Configuration mode, activates the process of re-authentication on all supplicants and for all ports.

Automatic 802.1X supplicant re-authentication can be set globally or for supplicants connected to individual ports.

By default, the re-authentication is disabled.

Command Syntax

```
device-name(config)#dot1x re-authenticate [UU/SS/PP]
```

Argument Description

UU/SS/PP	(Optional). Forces the re-authentication process on all supplicants for the specified port.

Example

```
device-name(config)#dot1x re-authenticate 1/1/1
```

Setting the Supplicant Authentication Timeout Period

The **dot1x timeout host** command, in Global Configuration mode, sets the authentication timeout period for the 802.1X supplicants. The **no** form of this command resets the period to its default value.

By default, the communication timeouts for the 802.1X supplicants is 30 second.

Command Syntax

```
device-name(config)#dot1x timeout host <time>
device-name(config)#no dot1x timeout host
```

Argument Description

time	The authentication timeout period in seconds, in the range <1-65535>.

Example

```
device-name(config)#dot1x timeout host 45
```

Setting the Period of Re-authentication

The **dot1x timeout re-authperiod** command, in Global Configuration mode, sets the number of seconds between re-authentication attempts. The **no** form of this command sets the re-authentication period to its default value.

This command affects the behavior of the switch only if periodic re-authentication is enabled. To enable the periodic re-authentication use the **dot1x re-authentication** command in Global Configuration mode.

By default, the period of re-authentication is 3600 second.

Command Syntax

```
device-name(config)#dot1x timeout re-authperiod <time>
device-name(config)#no dot1x timeout re-authperiod
```

Argument Description

time	The re-authentication period is a value in the range <1–4294967295>.

Example

```
device-name(config)#dot1x timeout re-authperiod 4200
```

Setting a Period of Time for the Quiet Timer

The **dot1x timeout quiet-period** command, in Global Configuration mode, sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the supplicant. The **no** form of this command resets the period to its default value.

When the switch cannot authenticate the supplicant, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the quiet-period value. The reason for failing to authenticate the supplicant may be an invalid password provided by the supplicant. You can provide the user a faster response time by specifying a number smaller than the default.

By default, the Quiet timer period is 60 second.

Command Syntax

```
device-name(config)#dot1x timeout quiet-period <time>
device-name(config)#no dot1x timeout quiet-period
```

Argument Description

time	The Quiet timer period is a value in range <1–65535>.

Example

```
device-name(config)#dot1x timeout quiet-period 120
```

Setting a Period for Communication Timeouts

The **dot1x timeout tx-period** command, in Global Configuration mode, sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request. The **no** form of this command resets the period to its default value of 30 seconds.

The supplicant responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits for a set period of time (known as the retransmission time) and then retransmits the frame.

By default, the period for communication timeouts is 30 second.

Command Syntax

```
device-name(config)#dot1x timeout tx-period <time>
device-name(config)#no dot1x timeout tx-period
```

Argument Description

time	The period for communication timeouts is a value in the range <1–65535>.

Example

```
device-name(config)#dot1x timeout tx-period 60
```

Setting the Unicast Supplicant Compatibility

The **dot1x unicast-client-compatibility** command, in Global Configuration mode, sets a mode that allows dot1x to work with supplicants, but without sending EAPOL packets to 802.1X group MAC addresses. The **no** form of this command sets a mode in which the dot1x does not work with supplicants and does not send EAPOL packets to 802.1X group MAC addresses.

By default, this mode is disabled.

NOTE Enabling this feature can affect the switch's performance.

Command Syntax

```
device-name(config)#dot1x unicast-client-compatibility
device-name(config)#no dot1x unicast-client-compatibility
```

802.1X Interface Configuration Commands

The table below lists the 802.1X interface configuration commands.

Table 34-5 802.1X Interface Configuration Commands

Command	Description
dot1x port-control	Sets the 802.1X particular control type for the specified port.
dot1x re-authenticate	Activates re-authentication for all supplicants that are connected to a specified port.
dot1x multiple-hosts	Sets 802.1X to Multiple-Hosts mode on a specified port.
dot1x control-direction permit-in-traffic	Sets the dot1x traffic mode to Bi-directional Traffic Control per port basis.

Setting the Control Type for a Specified Port

The **dot1x port-control c**ommand, in Interface Configuration mode, sets 802.1X control type for the specified port. The **no** form of this command disables the dot1x for the specified port.

The command **dot1x port-control** entered without specifying a control type, sets the switch to auto mode.

The default mode is force-authorized.

Command Syntax

```
device-name(config-if UU/SS/PP)#dot1x port-control [auto | force-
authorized | force-unauthorized]
```

```
device-name(config-if UU/SS/PP)#no dot1x port-control
```

Argument Description

auto	Sets 802.1X to auto mode on the specified port. Enables 802.1X on the specified interface with the default Single-Host mode.
force-authorized	Sets 802.1X in Force-Authorized mode on the specified port. Using this command is equivalent to stopping 802.1X.
force-unauthorized	Set 802.1X in Force-Unauthorized mode.

Example

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#dot1x port-control auto
```

Forcing Re-authentication for a Specified Port

The **dot1x re-authenticate** command, in Interface Configuration mode, activates re-authentication for all supplicants that are connected to the specified port.

Command Syntax

```
device-name(config-if UU/SS/PP)#dot1x re-authenticate
```

Example

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#dot1x re-authenticate
```

Setting 802.1X to Multiple-Hosts Mode for a Specified Port

The **dot1x multiple-hosts** command, in Interface Configuration mode, sets 802.1X to Multiple-Hosts mode on the specified port. The **no** form of this command sets the default 802.1X supplicant mode on a specified port.

By default, the 802.1X supplicant mode on a specified port is Single-Host mode.

Command Syntax

```
device-name(config-if UU/SS/PP)#dot1x multiple-hosts [per-mac-mode
max-clients [<number>]]
device-name(config-if UU/SS/PP)#no dot1x multiple-hosts [per-mac-mode
max-clients [<number>]]
```

Argument Description

per-mac-mode	(Optional). Sets 802.1X in Multiple-Hosts / Per-MAC-Authorization on this port.
max-clients	(Optional). Specifies the maximum number of supplicants for this port.
number	(Optional) The maximum number of supplicants allowed for this port. If no value is specified, the command resets the number of allowed clients to the default value of 0. The range is <1-500>.

Example

```
device-name(config)#interface 1/1/1
device-name(config-if 1/1/1)#dot1x multiple-hosts per-mac-mode max-
clients 2
```

Setting the Traffic Mode

The **dot1x control-direction stop-in-traffic** command, in Interface Configuration mode, sets the dot1x traffic mode to Bi-directional Traffic Control. The **no** form of this command sets the dot1x traffic mode to "Unidirectional traffic control".

By default, the Bi-directional Traffic Control is enabled.

Command Syntax

```
device-name(config)#dot1x control-direction stop-in-traffic
device-name(config)#no dot1x control-direction stop-in-traffic
```

Displaying the 802.1X Information

The table below lists the available 802.1X display commands.

Table 34-6 802.1X Display Commands

Command	Description
dot1x	Displays the 802.1X authentication setting globally and on a per-port basis.
show dot1x	Displays information regarding 802.1X authentication.
show dot1x radius	Displays all RADIUS servers that are configured
show dot1x interface	Displays the 802.1X for a specific port
show dot1x hosts	Display 802.1X information for all supplicants.

Displaying 802.1X Authentication Information

The **show dot1x** command, in Privileged (Enable) mode, displays information regarding 802.1X authentication.

Command Syntax

```
device-name#show dot1x
```

Example

```
device-name#show dot1x

ReAuthentication                = ENABLED
ReAuthentication timer          = 25 sec
Unicast-clients compatibility   = OFF
Radius timeout                  = 50 sec
Supplicant timeout              = 30 sec
Tx-period timeout               = 5 sec
Quiet period                    = 390 sec
================================================================
Port  Hosts Auth  UnAuth  AuthMethod AuthType        ControlDirection
----------------------------------------------------------------
```

```
1/1/1    0       0       0       Auto      Per MAC          In
1/1/5    1       1       0       Auto      Single           Both
```

Displaying the Configured RADIUS Servers

The **show dot1x radius** command, in Privileged (Enable) mode, displays all RADIUS servers that are configured.

Command Syntax

```
device-name#show dot1x radius [statistic]
```

Argument Description

statistic	(Optional). Display statistic information for the configured RADIUS servers

Example 1

```
device-name#show dot1x radius
Configured RADIUS Servers       1
Retransmit count                2
Timeout                         50 sec
DeadTime                        0 sec
==============================================================================
ID      IP Address      Port    Status  Key             Status Time
------------------------------------------------------------------------------
1       192.168.0.40    1812    ALIVE   configured      00:55:42
```

Example 2

```
device-name#show dot1x radius statistic

RADIUS server [192.168.0.40:1812]:
  Sent Packets:
    RADIUS Request:             270
  Received Packets:
    RADIUS Accept:              135
    RADIUS Reject:              0
    RADIUS Challenge:           135
    RADIUS Unknown:             0
```

Displaying the 802.1X for a Specific Port

The **show dot1x interface** command, in Privileged (Enable) mode or the **dot1x** command in Interface Configuration mode, displays the 802.1X for a specific port.

Command Syntax

```
device-name#show dot1x interface UU/SS/PP [detailed | statistic]

device-name(config-if UU/SS/PP)#dot1x
```

Argument Description

UU/SS/PP	Interface's unit/slot/port.
detailed	Displays detailed information for every supplicant on a specific port.
statistic	Displays statistic information for a specific port.

Example 1

```
device-name#show dot1x interface 1/1/5

Control Direction        = Both
Authentication Method    = Auto
Authentication Type      = Single Host
Host Limit               = Unlimited
Hosts                    = 1
Authorized Hosts         = 1
UnAuthorized Hosts       = 0
================================================================================
MAC                 Vlan State      RadID   Session time  ReAuth
--------------------------------------------------------------------------------
00:40:95:31:80:6D 2 Authenticated   1       00:28:12      00:00:01
```

Example 2

```
device-name#show dot1x interface 1/1/5 statistic

Total OUT EAPOL Frames                  256
  EAPOL Packet ID Request               86
  EAPOL Packet Request                  85
  EAPOL Packet Success                  85
  EAPOL Packet Fail                     0

Total OUT Retransmit Radius Frames      170
Total IN EAP Radius Frames              170

Total IN EAPOL Frames                   170
  EAPOL Start                           0
  EAPOL LogOff                          0
  EAPOL Packet ID Response              85
  EAPOL Packet Response                 85
  EAPOL Key                             0
  EAPOL ASF Alert                       0
  EAPOL Unknown                         0
  EAPOL Broken                          0

Last EAP Version Received:              1
Last EAPOL Packet Received from:        [00:40:95:95:80:31]]
```

Example 3

```
device-name(config-if 1/1/5)#dot1x

Control Direction        = In
Authentication Method    = Auto
Authentication Type      = Multiple Hosts
Host Limit               = Unlimited
Hosts                    = 1
Authorized Hosts         = 1
UnAuthorized Hosts       = 0
```

Displaying the 802.1X Information for all Supplicants

The **show dot1x hosts** command, in Privileged (Enable) mode, displays the 802.1X information for all supplicants.

Command Syntax

```
device-name#show dot1x hosts
```

Example

```
device-name#show dot1x hosts
================================================================================
MAC          Vlan Port     State        RadID  Session time  ReAuth
--------------------------------------------------------------------------------
00:40:95:31:80:6D 2  1/1/5  Authenticated   1    00:59:02    00:00:01
```

Debugging 802.1X

The table below lists the 802.1X debugging commands.

Table 34-7 802.1X Debugging Commands

Command	Description
debug dot1x	Enables specific 802.1X debugging.
debug dot1x authsm	Enables the authenticator state machine debugging.
debug dot1x basm	Enables the backend state machine debugging.
debug dot1x packet	Enables a specific packet debugging
show debug dot1x	Displays the status of the 802.1X debug actions that are currently activated in the switch.

Enabling Debuggig

The **debug dot1x** command, in Privileged (Enable) mode, enables specific 802.1X debugging. The **no** form of this command turns off the 802.1X debugging.

The dot1x debug commands will not be saved after reload.

By default, the debug is disabled.

Command Syntax

```
device-name#debug dot1x [all | core | radius | reauthsm]
device-name#no debug dot1x [all | core | radius | reauthsm]
```

Argument Description

all	Debug the whole 802.1X process.
core	Debug the 802.1X core process.
radius	Debug RADIUS events.
reauthsm	Debug re-authentication.

Authenticator State Machine Debugging

The **debug dot1x authsm** command, in Privileged (Enable) mode, enables the authenticator state machine debugging. The **no** form of this command disables this debugging state.

The dot1x debug commands will not be saved after reload.

By default, the debug is disabled.

Command Syntax

```
device-name#debug dot1x authsm {event | status | timers}
device-name#no debug dot1x authsm {event | status | timers}
```

Argument Description

event	Debug state machine events.
status	Debug state machine status.
timers	Debug state machine timers.

Backend State Machine Debugging

The **debug dot1x basm** command, in Privileged (Enable) mode, enables the backend state machine debugging. The **no** form of this command disables this debugging state.

The dot1x debug commands will not be saved after reload.

By default, the debug is disabled.

Command Syntax

```
device-name#debug dot1x basm {event | status | timers}
device-name#no debug dot1x basm {event | status | timers}
```

Argument Description

event	Debug backend state machine events.
status	Debug backend state machine status.
timers	Debug backend state machine timers.

Specific Packet Debugging

The **debug dot1x packet** command, in Enable Mode, debugs 802.1X related packets. The **no** form of this command turns off the packet debugging.

The dot1x debug commands will not be saved after reload.

By default, the debug is disabled.

Command Syntax

```
device-name#debug dot1x packet {all | eapol | radius} {recv | send}
[detail]
device-name#no debug dot1x packet {all | eapol | radius} {recv |
send} [detail]
```

Argument Description

all	Debug all 802.1X related packets, no detail.
eapol	Debug EAPOL packets.

radius	Debug RADIUS packets.
recv	Debug packets sending and receiving.
send	Debug packets receiving.
detail	Debug packets sending.

Displaying the 802.1X Debugging

The **show debug dot1x** command, in Privileged (Enable) mode, displays the debug status for the 802.1X. The debug commands can help the network manager to monitor a session as it proceeds on the switch.

Command Syntax

```
device-name#show debug dot1x
```

Example

```
device-name#show debug dot1x

PBA core debugging is on: 802.1X core process,Re-Authentication
process
PBA Authenticator State Machine debugging is on:
   status,events,timers
PBA Backend State Machine debugging is on:
   status,events,timers
PBA RADIUS debugging is on: packet send,packet receive,events,
PBA EAPOL debugging is on: packet send,packet receive
```

Configuration Example

1. Set the RADIUS server and specify the IP address, key, username, password and AAA authentication:

```
device-name#configure terminal
device-name(config)#radius-server host 9.0.0.26
device-name(config)#radius-server key hello
device-name(config)#username batm password a1h8RRzG11d4U
device-name(config)#aaa authentication login default radius local
```

2. Configure port 1/1/6 of the Authenticator for authorization, setting it to auto authorization mode:

```
device-name(config)#interface 1/1/6
device-name(config-if 1/1/6)#dot1x port-control auto
```

Related Commands

The table below shows the 802.1X-related commands.

Table 34-8 802.1X-Related Commands

Command	Description	Described in
radius-server host	Defines the remote RADIUS server.	Understanding and Configuring Remote Authentication Dial In User Service (RADIUS)
radius-server key	Specifies the password used between the router and the RADIUS server.	Understanding and Configuring Remote Authentication Dial In User Service (RADIUS)
username	Adds a username and an associated password to the local authentication database.	Understanding and Configuring Remote Authentication Dial In User Service (RADIUS)
aaa authentication login default	Specifies the default login authentication method.	Understanding and Configuring Remote Authentication Dial In User Service (RADIUS)

35. Built-In Self Test (BIST)

Overview

The Built-in Self Test (BIST) performs a set of basic tests of switch hardware and of its configuration validity.

Startup BIST - The BIST is performed automatically on startup. The results are summarized on the terminal before the switch banner.

BIST by request - At any time a user may request BIST execution, by using a CLI command.

The current BIST status may be read and cleared by using CLI commands.

When the BIST detects a failure in any of the tests, it causes the Status LED indicator to blink.

Table 35-1 summarizes the BIST tests for the ESB26 switch.

Table 35-1 Description of the Built-in Tests

Test	Description
CPU Notify RAM Test	On boot, the entire DRAM is tested. This test is run once at startup.
CPU Interface Test	Checks the existence of the UART (register write/read operation). Only COM1 is checked.
Data Buffer Test	Checks the integrity of NVRAM database.

NOTES

1. To display BIST failure results, use the show self-test command in Privileged mode.
2. To display all BIST results, use the show self-test full command in Privileged mode.
3. To invoke a BIST by Request at any time the switch is running, use the self-test command in Privileged mode.

Startup Execution of BIST

When the power is turned on, the switch executes a startup BIST. The switch reports a summary of the results on the terminal. The results are either **Passed** or **Failed**, as in the following report is example:

```
ESB26#self-testProcessingBIST by request... CPUCore Test        :CPUNotify
RAM Test  :CPUInterface Test   :    UART Existence     - PassedTestingSwitch
Core  :    Crossbar Existence - PassedOn-boardPower Test  :    On-board
Power PHY - Passed    On-board Power CPU - Passed    On-board Power OC  -
PassedTemperatureTest     :    Temperature        - PassedBroadcastLimit
Test :    Broadcast Limit    - Passed
```

BIST Commands

The available BIST commands are summarized in Table 35-2.

Table 35-2 BIST Commands

Command	Description
self-test	Initiates BIST by Request.
show self-test	Issues a report on the current built-in test status (obtained by the last BIST).

Description of Commands

self-test

The **self-test** command, in Privileged (Enable) mode, initiates BIST by Request. All BIST tests are executed except for **CPU Notify RAM Test** (not allowed because it resets the memory). Execution of BIST by Request updates the statuses of test results. The command issues a full BIST status report (except for the **CPU Notify RAM Test**).

Command Syntax

```
device-name#self-test
device-name#no self-test
```

Example

```
device-name#self-test
Processing BIST by request...

CPU Core Test        :
    CPU Validation     - Passed
CPU Notify RAM Test  :
    RAM Validation     - Passed
CPU Interface Test   :
    UART Existence     - Passed
Testing Switch Core  :
    Crossbar Existence - Passed
On-board Power Test  :
```

```
    On-board Power PHY = Passed
    On-board Power CPU = Passed
    On-board Power OC  - Passed
Temperature Test     :
    Temperature        - Passed
```

show self-test

The **show self-test** command, in Privileged (Enable) mode, issues a report on the current built-in test status (obtained by the last BIST).

If **full** is specified, the command issues a full report, comprising the status (**Passed/Failed**) of each test.

If **full** is not specified, the command issues a brief report, comprising:

- a notification stating whether problems were encountered;
- items that failed (if any), with their (**Failed**) statuses.

Command Syntax

```
device-name#show self-test [full]
```

Examples

1. The following example displays a brief report about the current BIST status, when all tests resulted with Passed statuses:

```
device-name#show self-test
No problem encountered by BIST
```

2. The following example displays a brief report about the current BIST status, when the **Crossbar Existence** test resulted with **Failed** status:

```
device-name#show self-test
Problem encountered by BIST
---------------------------

CPU Interface Test  :
    UART Existence          - Passed
```

3. The following example displays a full report about the current BIST status:

```
device-name#show self-test full

Checking current BIST status...

device-name#self-test
Processing BIST by request...

CPU Core Test        :
    CPU Validation     - Passed
CPU Notify RAM Test  :
    RAM Validation     - Passed
CPU Interface Test   :
    UART Existence     - Passed
Testing Switch Core  :
    Crossbar Existence - Passed
```

```
On-board Power Test :
    On-board Power PHY - Passed
    On-board Power CPU - Passed
    On-board Power OC  - Passed
Temperature Test     :
    Temperature        - Passed
```

36. Diagnostic Tests

ESB26 Diagnostics-Related Commands

ESB26 device has an integrated procedure for self-testing and diagnostics. Diagnostic tests check the proper operation and integrity of certain parts of device. The self-testing is usefull for network administators, for troubleshooting and proper maintenance of the devices. The diagnostic module includes the following validation tests:

- **NVRAM contents**

  Validates the integrity and proper functionality of NVRAM contents. The validation includes application images CRC check, Java-image CRC check, Startup-config CRC check, script file system structure check and serial prom validation.

- **CPU functionality**

  Validates the proper operation of Central Processing Unit.

- **Switch chip-set functionality**

  Validates the proper back-plane operation.

- **R/W-memory functionality**

  Validated the proper operation of read/write RAM.

- **LAN-ports functionality**

  Verifies the proper operation of LAN-ports using loopback interface.

The Diagnostics-Related Commands

The table below lists the available diagnostics-related commands.

Table 36-1 Diagnostics-Related Commands

Command	Description
self-test	Enters the self-test mode.
show test-results	Displays all test results.
test cpu	Tests the CPU functionality.
test nvm-contents application	Validates the application image.
test nvm-contents java-image	Validates the View Agent Image.

test nvm-contents loader	Validates the loader image.
test nvm-contents prom-access	Validates the operability of EPROM.
test nvm-contents script-file-system	Validates the script file system.
test nvm-contents startup-configuration	Validates the startup configuration.
test switch-core	Validates the switch core.
test ram	Tests the RAM.
test ports	Checks all ports.
test all	Performs all tests.
clear test-results	Deletes all test results.
test end	Ends the self-test mode.

self-test

The **self-test** command, in System mode, enters the self-test mode for performing diagnostics and testing the device functionality.

Command Syntax

```
device_name(show system)#self-test
device_name(self-test)#
```

test cpu

The **test cpu** command, in self-test mode, validates the proper operation of Central Processing Unit.

Command Syntax

```
device_name(self-test)#test cpu
```

Example

```
device_name(self-test)#test cpu

  CPU validation --> OK
```

test nvm-contents application

The **test nvm-contents application** command, in self-test mode, performs diagnostic of the primary/secondary application image. This diagnostic is performed by verifying the correct CRC of application images saved in internal Flash memory.

Command Syntax

```
device_name(self-test)#test nvm-contents application (primary|secondary)
```

Argument Description

primary	The primary application image
secondary	The secondary application image

Example

```
device_name(self-test)#test nvm-contents application primary

Image Size = 0x2D7313
CRC Value = 0xD78F9816
Application image in NVM is OK
```

test nvm-contents java-image

The **test nvm-contents java-image** command, in self-test mode, performs diagnostics of the java image. This diagnostic is performed by verifying the correct CRC of the java image in internal Flash memory.

Command Syntax

```
device_name(self-test)#test nvm-contents java-image
```

Example

```
device_name(self-test)#test nvm-contents java-image

Image Size = 0x200000
CRC Value = 0x9A4109E5
Java image in NVM is OK
```

test nvm-contents loader

The **test nvm-contents loader** command, in self-test mode, performs diagnostics of the Boot loader image. This diagnostic is performed by verfying the correct CRC of the boot loader image.

Command Syntax

```
device_name(self-test)#test nvm-contents loader
```

Example

```
device_name(self-test)#test nvm-contents loader

Image Size = 0x7bf00
CRC Value = 0x0495d8b3
Loader in NVM is OK
```

test nvm-contents prom-access

The **test nvm-contents prom-access** command, in self-test mode, performs diagnostic of serial EEROM. This diagnostic is performed by checking the serial-prom label.

Command Syntax

```
device_name(self-test)#test nvm-contents prom-access
```

Example

```
device_name(self-test)#test nvm-contents prom-access

Validation of PROM passed OK
```

test nvm-contents script-file-system

The **test nvm-contents script-file-system** command, in self-test mode, performs diagnostics of script file system. This diagnostic is performed by checking the integrity of control structure of the script file system located on the internal Flash memory.

Command Syntax

```
device_name(self-test)#test nvm-contents script-file-system
```

Example

```
device_name(self-test)#test nvm-contents script-file-system

Script file system in NVM is OK
```

test nvm-contents startup-configuration

The **test nvm-contents startup-configuration** command, in self-test mode, performs diagnostics of the startup configuration file saved in internal Flash memory. This diagnostic is performed by checking for correct CRC of the startup-configuration.

Command Syntax

```
device_name(self-test)#test nvm-contents startup-configuration
```

Example

```
device_name(self-test)#test nvm-contents startup-configuration

Startup configuration in NVM is OK
```

test switch-core

The **test switch-core** command, in self-test mode, performs diagnostics of the switch chip-set functionality and validates the proper back-plane operation.

Command Syntax

```
device_name(self-test)#test switch-core
```

Example

```
device_name(self-test)#test switch-core

Switch core validation --> OK
```

test ram

The **test ram** command, in self-test mode, validates the random access memory. During the test, the normal switch operation is interrupted and the device enters Debug self-test switch mode.

Command Syntax

```
device_name(self-test)#test ram
```

Example

```
device_name(self-test)#test ram

Normal switch operation will be interrupted. Proceed ? [y/n] : y



Verifying validity of primary application.....OK



Start primary application...
Press Escape to stop the test

Data Bus Test: Walking One --> OK
Data Bus Test: Walking Zero --> OK

Address Bus Test: Walking One --> OK
Address Bus Test: Walking Zero --> OK

RAM Device Test : 100% --> OK

Entering into self-test switch mode. Please wait...
```

test ports

The **test ports** command, in self-test mode, checks the normal operation of all ports using internal loopback. During the test, the normal switch operation is interrupted and the device enters Debug self-test switch mode.

Command Syntax

```
device_name(self-test)#test ports
```

Example

```
device_name(self-test)#test ports

To perform the test, the switch must first pass to debug mode
Normal switch operation will be interrupted. Proceed ? [y/n] : y



Verifying validity of primary application.....OK
```

```
Start primary application...

Entering into self-test switch mode. Please wait...

All ports --> OK
```

test all

The **test all** command, in self-test mode, performs all tests subsequiently.

Command Syntax

```
device_name(self-test)#test all
```

Example

```
device_name(self-test)#test all

Normal switch operation will be interrupted. Proceed ? [y/n] : y

Testing CPU:
CPU validation --> OK

Testing Switch Core:
Switch core validation --> OK

Testing loader:
Image Size = 0x7bf00   CRC Value = 0x0495d8b3
Loader in NVM is OK

Testing application:
Image Size = 0x2D7313   CRC Value = 0xD78F9816
Application image in NVM is OK
Testing startup configuration:
Startup configuration in NVM is OK

Testing script file system:
Script file system in NVM is OK

Testing java image:
Image Size = 0x200000   CRC Value = 0x9A4109E5
Java image in NVM is OK

Testing PROM access:
Validation of PROM passed OK
Testing RAM:



Verifying validity of primary application.....OK



Start primary application...
Press Escape to stop the test

Data Bus Test: Walking One --> OK
Data Bus Test: Walking Zero --> OK
```

```
Address Bus Test: Walking One --> OK
Address Bus Test: Walking Zero --> OK

RAM Device Test : 100% --> OK

Entering into self-test switch mode. Please wait...
All ports --> OK
```

clear test-results

The **clear test-results** command, in self-test mode, clears the last self-test results.

Command Syntax

```
device_name(self-test)#clear test-results
```

Example

```
device_name(self-test)#clear test-results

device_name(self-test)#show test-results
  CPU Core Test    : Not performed
  Switch Core Test: Not performed
  NVM Data Test    : Not performed
  RAM Test         : Not performed
  Ports Test       : Not performed
```

show test-results

The **show test-results** command, in self-test mode, displays all test results that have been performed.

Command Syntax

```
device_name(self-test)#show test-results
```

Example

```
device_name(self-test)#show test-results

  CPU Core Test    : Passed
  Switch Core Test: Passed
  NVM Data Test    : Passed
  RAM Test         : Passed
  Ports Test       : Passed
```

test end

The **test end** command, in Debug self-test mode, exits the Debug self-test mode that the switch has been entered to after performing RAM or port tests, and returns to normal mode.

Command Syntax

```
device_name(self-test)#[DBG] test end
```

Example

```
device_name(self-test)#[DBG] test end

Return to normal switch operation. Procceed ? [y/n] : y

Verifying validity of primary application.....OK


Start primary application...

Return to normal switch operation. Please wait...


device_name(show system)#
```

37. DNS Resolver

Introduction

The Domain Name System (DNS) is the means by which Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. There is probably a DNS server within close geographic proximity to your access provider that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

Figure 37-1 is an example for the DNS operation. The client enters a domain name (www.domainname.com) into his browser. The browser contacts the Client's ISP for the IP address of the domain name. The ISP first tries to answer by itself using "cached" data. If the answer is found it is returned. Since the ISP isn't in charge of the DNS, and is just acting as a "DNS relay", the answer is marked "non-authoritative". If the answer is not found or if it is too old (past the TTL), the ISP DNS contacts the nameservers for the domain directly for the answer. If the nameservers are not known, the ISP looks for the information at the 'root servers', or 'registry servers'. For com/net/org, these start with a.gtld-servers.net.

Feature Overview

You can define up to three DNS servers. If a query to the primary address fails to be resolved after three attempts, the next gateway address is queried. This process continues for each defined gateway address until the query is resolved or when all the queries have failed. The order in which the default gateway addresses are polled is the same as the order in which you enter them.

DNS is a distributed database with which you can map host names to IP addresses through the DNS protocol from a DNS server. When you configure DNS on the switch, you can substitute the host name for the IP address with the **ping** and **traceroute** commands in Privileged (Enable) mode.

The BiNOS supports a cache mechanism for names that are already resolved. If a resolve query arrives at the switch, the DNS Resolver first searches the requested name in that cache. If it does not find any match, the DNS Resolver delivers the query to the DNS server. The TTLs (time to live) of those cache entries are extracted from the Resource Record (RR) of the server's response.

To use DNS, you must have a DNS name server present on your network.

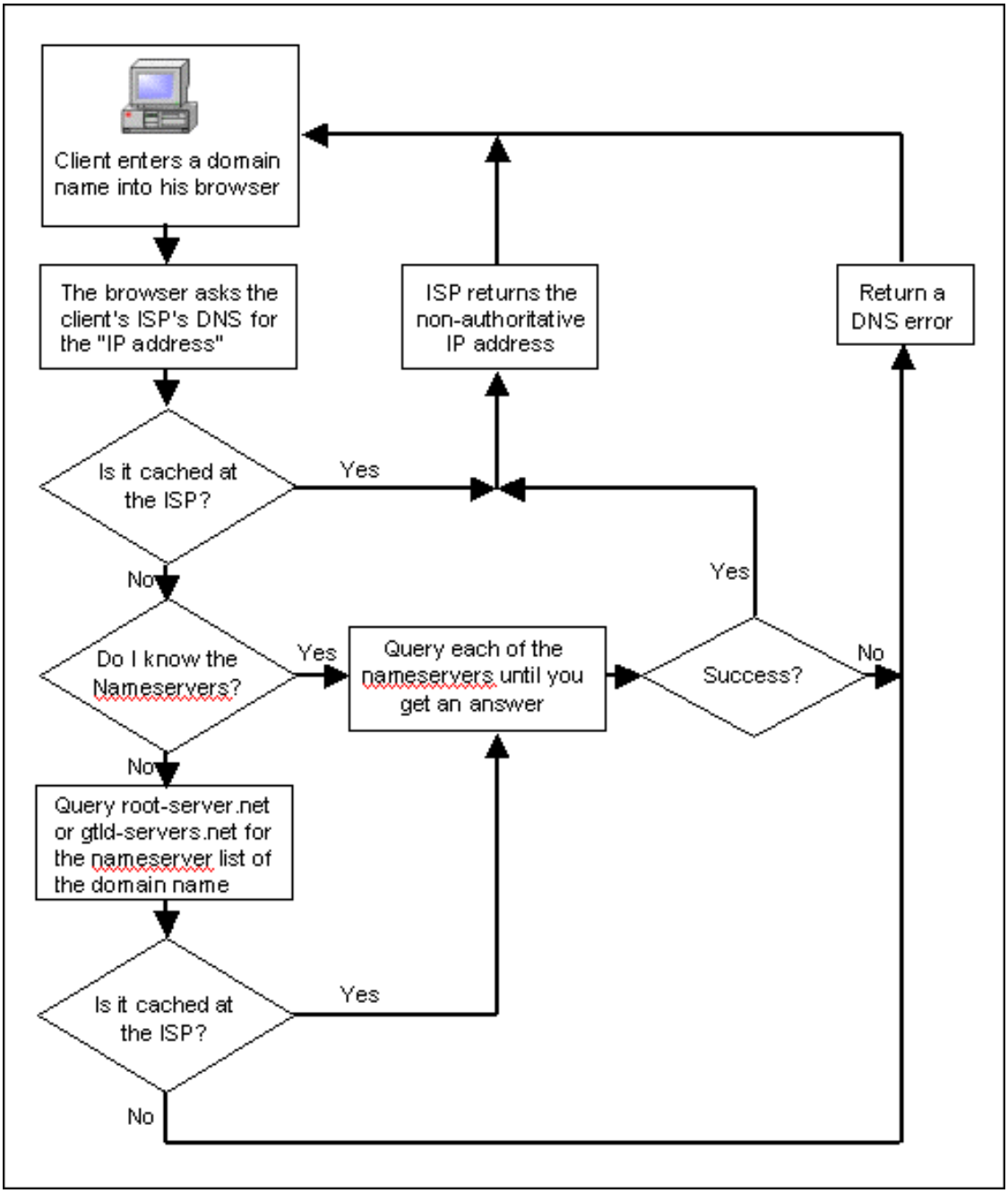


Figure 37-1: Simplified Example of How DNS Works

Supported Standards, MIBs and RFCs

Standards

No standards are supported by this feature.

MIBs

No MIBs are supported by this feature.

RFCs

RFC 1034, *Domain Names – Concepts and Facilities*

RFC 1035, *Domain Names – Implementation and Specification*

Default DNS Resolver Configuration

Table 37-1 shows the default DNS Resolver configuration.

Table 37-1 DNS Resolver Default Configuration

Parameter	Default Value
DNS servers	None specified

Configuring and Displaying DNS Resolver

Table 37-2 lists the DNS Resolver commands.

Table 37-2 DNS Resolver Commands

Command	Description
ip dns server	Specifies the IP address of one or more DNS servers.
show ip dns	Displays the current configuration of the DNS Resolver.

Setting DNS Server

The **ip dns server** command, in Global Configuration mode, specifies the IP address of one or more DNS servers. Up to three DNS servers can be added.

The first IP address is the primary gateway address and all others are secondary addresses.

Command Syntax

```
device-name(config)#ip dns server A.B.C.D
device-name(config)#no ip dns server A.B.C.D
```

Argument Description

A.B.C.D	The IP address of the DNS server.

Displaying the DNS Resolver Configuration

The **show ip dns** command, in Privileged (Enable) mode, displays the current configuration of the DNS Resolver.

Command Syntax

```
device-name#show ip dns
```

Configuration Example

In the following example, the first IP address in the **ip dns server** command becomes the primary gateway address and all others are secondary addresses. Because IP address 201.98.7.15 is the last address listed, it is also the last address consulted to resolve a query.

```
device-name(config)#ip dns server 209.157.22.199
device-name(config)#ip dns server 205.96.7.15
device-name(config)#ip dns server 201.98.7.15
```

The following command displays the DNS configuration:

```
device-name(config)#end
device-name#show ip dns

DNS Resolver configuration:
First  DNS server 209.157.22.199
Second DNS server 205.96.7.15
Third  DNS server 201.98.7.15
```

Related Commands

Table 37-3 shows the DNS Resolver related commands.

Table 37-3 DNS Resolver Related Commands

Command	Description	Described in
ping	Allows pinging to another unit (e.g. switch, PC, router).	Getting Started, View Mode and Privileged Mode
traceroute	Traces routing path.	Getting Started, View Mode and Privileged Mode

APPENDIX
Loader, Sysloader and Dual Boot

Overview

ESB26 has two separate special startup modes, called "Loader" and "Sysloader". They can be entered rignt after turning on or resetting the switch. They both have almost the same purpose and differ only in the commands provided and the way the commands function. The Loader/Sysloader modes are designed for:

- auto-starting the routing switch's application;
- configuration of basic parameters;
- rescue tools in case of routing switch inoperability;
- memory exploring tools.

When starting, the system counts down a few seconds, allowing the user an entry point into Loader/Sysloader. During that time, pressing any key enters Sysloader mode and pressing any key enters Loader mode. The switch then goes into the respective Loader/Sysloader interactive mode, requests login password, and starts a CLI. If no key is pressed, the auto-startup of the switch application is performed.

The commands available in each of these startup modes and their use are covered in detail below.

Loader

Commands Summary

Table APPENDIX-1 Initial CLI Mode Commands

more	Filters command output.
config	Sets starting defaults (entrance into configuration mode).
download	Downloading SW components to NVRAM.
exit	Exits current mode and goes back to previous mode (from this mode – logout as in command quit).
help	Description of the interactive help system.
list	Prints command list.
ip-address	Sets IP address of the loader.
memory	Accesses the memory debug tools (entrance into memory mode)

quit	Disconnects and logs out.
start	Starts execution of switch application.
copy	Files transfer to the target base.
version	Displays the switch's model and loader version.
manufacturing-details	Displays manufacture details.

Table APPENDIX-2 Configuration Mode Commands

more	Filters command output.
mac-address	Sets MAC address of switch.
clean	Rough-cleans the NVRAM database.
end	Ends current mode and change to enable mode.
exit	Exits current mode and down to previous mode.
help	Descriptions of the interactive help system.
ip-address	Configures IP address of the loader. (Used for manufacturing purposes only.)
list	Prints command list.
manufacturing-details	Configures manufacture details.
quit	Disconnects and logs out.

Table APPENDIX-3 Board Configuration Commands

more	Filters command output
assembly-number	Configures the assembly part of the manufacturing serial number
board-revision	Configures the board revision part of the manufacturing serial number
board-sub-revision	Configures the of the board sub-revision part of the manufacturing serial number
clear	Clearя details about board manufacturing
end	Ends current mode and change to initial mode.
exit	Exits current mode and down to previous mode
help	Descriptions of the interactive help system
list	Prints command list
quit	Disconnects and logs out.

serial-number	Configures the manufacturing serial numberл
show	Displays board manufacturing details.

Table APPENDIX-4 Memory Mode Commands

more	Filter command output
copy	Copy block of memory
display	Display block of memory
end	End current mode and change to initial mode.
exit	Exit current mode and down to previous mode
fill	Fill block of memory by value
help	Description of the interactive help system
list	Print command list
quit	Disconnect and logout

Description of Commands

Commands for Downloading Software and Starting the Switch Manually

To start the execution of the switch's application, use the following command:

start application

The **start application** command, in Loader mode, terminates the loader and starts the execution of the switch's application.

Command Syntax

```
Loader>start application [safe]
```

Argument Description

safe	(Optional) Start in safe mode with default configuration.

NOTE The optional argument *safe* is used for technical support only.

Example

```
Loader>start application
Starting switch application from flash, please wait...
```

```
////////////////////////////////////////////////////////////
//                                                        //

// Switch model : NOKIA ESB26                            //
//  SW version   : 3.3.0 created Oct 21 2003 - 14:59:16   //
//                                                        //
////////////////////////////////////////////////////////////
User Access Verification
Password:
```

download application

The **download application** command, in Loader mode, copies the switch's application from a source computer to the switch's permanent storage memory, through a console connection by X-modem transfer.

When you **type** the download command on the console, the switch waits for a file transfer and periodically sends NAKs (negative acknowledgments) to the console. These appear on the console screen as garbage characters.

The transfer starts in an X-modem format.

Upon completion of the transfer, the switch checks if the received file is a valid switch application code. If it is, the received image is stored in the internal FLASH memory.

This role of the **download** command is to provide a rescue solution in case the switch becomes inoperable and a new application image cannot be received by the TFTP transfer.

Command Syntax

```
Loader>download application
```

Example

```
Loader>download application
XMODEM application download to flash 0
XMODEM Receive: Waiting for Sender
Image Size = 0xBD552 CRC Value = 0x691181F3
Saving application code to FLASH bank 0....Success.
Loader>
```

manufacturing details

The **manufacturing-details** command, in Loader mode, displays manufacture details.

Command Syntax

```
Loader>manufacturing-details
```

Example

```
Loader>manufacturing-details
Serial number : 13456 9
Assembly No : 1234567
HW revision : 123
HW subrevision : 123
Loader>
```

Commands to Configure the Switch from the Loader

The table below summarizes the CLI commands available upon entering Loader mode. The commands are described in the subsections that follow.

Table APPENDIX-5 Loader Configuration Commands

Command	Description
config	Switches from Loader initial to Loader configuration mode.
mac-address	Displays or changes the switch's MAC address.
clean startup-configuration	Sets the startup configuration database in the permanent storage memory to the default values.
clean log-history	Cleans all history records.
ip-address	Configures IP address of the loader. (Used for manufacturing purposes only.)

config

The **config** command, in Loader Configuration mode, switches the CLI from initial mode to Loader configuration mode.

Example

```
Loader>config
Loader(config)#
```

mac-address

The **mac-address** command, in Loader Configuration mode, displays or changes the MAC address of the switch. If no optional parameter is entered, the current MAC address is displayed.

Command Syntax

```
Loader(config)#mac-address [HH:HH:HH:HH:HH:HH]
```

Argument Description

HH:HH:HH:HH:HH:HH	The switch MAC address.

Examples

1. Displaying the switch's current MAC address:

```
Loader(config)#mac-address
Current base MAC Address of switch = 00:A0:12:1B:00:60
OutBand MAC Address (base + 1) = 00:A0:12:1B:00:61
```

2. Assigning new MAC address to the switch. The response indicates that the new MAC address is accepted and stored in the switch's memory.

```
Loader(config)#mac-address 00:a0:12:07:0f:78
New MAC Address of switch = 00:A0:12:07:0F:78
```

clean startup-configuration

The **clean startup-configuration** command, in Loader Configuration mode, sets the startup configuration database in the permanent storage memory to the default values.

Command Syntax

```
Loader(config)#clean startup-configuration
```

clean log-history

The **clean log-history** command, in Loader Configuration mode, erases all the log history records.

Command Syntax

```
Loader(config)#clean log-history
```

ip-address

The ip-address command, in Loader Configuration mode, changes the IP address of the loader. This IP address is used only for manufacturing purposes. The change is effective after restarting the switch.

Command Syntax

```
Loader(config)#ip-address [IP Address]
```

Argument Description

IP Address	The switch MAC address.

Example

```
Loader(config)#ip-address
A.B.C.D[/M]   Set IP address (optionally with num. of subnet mask
bits)
Loader(config)#ip-address 192.168.0.12/24

New loader IP address = 192.168.0.12, subnet mask = ffffff00
    WARNING: New IP address will take effect
             after restart of the switch
```

manufacturing-details

The **manufacturing-details** command is password protected and is used for manufacturing purposes only.

Command Syntax

```
Loader(config)#manufacturing-details
```

show

The **show** command, in Board Configuration mode, displays the manufacturing serial board number and manufacturing details .

Command Syntax

```
Loader(board)> show
```

Example

```
Loader(board)>manufacturing-details
Serial number : 134569
Assembly No : 1234567
HW revision : 123
HW subrevision : 123
```

Memory Debug Tools

The table below summarizes the CLI commands available at the Loader memory mode. The commands are described in the subsections that follow.

Table APPENDIX-6 Loader Memory Mode Configuration Commands

Command	Description
memory	Switches from Loader initial to Loader memory debug tools mode.
copy	Copies a block of memory.
display	Displays a block of memory.
fill	Fill a block of memory with a specified value.

memory

The **memory** command, in Loader mode, switches the CLI from Loader mode to Loader memory.

Command Syntax

```
Loader>memory
```

The command will be followed by the following prompt line:

```
Loader(memory)#
```

copy

The **copy** command, in Loader Memory mode, copies a block of memory that is specified by block-length from the specified source address to the specified destination address.

Command Syntax

```
Loader(memory)#copy SRC_ADDR DST_ADDR BLK_LEN
```

Argument Description

SRC_ADDR	Hexadecimal source address (optionally prefixed with 0x).
DST_ADDR	Hexadecimal destination address (optionally prefixed with 0x).
BLK_LEN	Hexadecimal or decimal block length (Use the 0x prefix for hexadecimal number).

Example

```
Loader(memory)#copy 0xF0000000 0xA0000000 10
Loader(memory)#
```

display

The **display** command, in Loader Memory mode, displays a block of memory, optionally specified by start address and block length in bytes.

Without any arguments, the command repeats the previous display, if any, or the default (after reload, the start address and block length are 0 and 256 respectively by default). If only the start address is specified, the previous or default block length is repeated.

Command Syntax

```
Loader(memory)#display [ST_ADDR [BLK_LEN]]
```

Argument Description

ST_ADDR	Hexadecimal start address (optionally prefixed with 0x).
BLK_LEN	Hexadecimal or decimal block length (Use 0x prefix for hexadecimal number).

fill

The **fill** command, in Loader Memory mode, fills a block of memory by value.

Command Syntax

```
Loader(memory)#fill ST_ADDR BLK_LEN VALUE
```

Argument Description

ST_ADDR	Hexadecimal start address (optionally prefixed with 0x).
BLK_LEN	Hexadecimal or decimal block length (Use 0x prefix for hexadecimal number).
VALUE	Hexadecimal byte value to fill (optionally prefixed with 0x).

Sysloader and Dual Boot

Dual Boot

ESB26 supports the dual boot feature that allows booting from either of two available images. Dual boot is used when you want to store two different software versions on the device. When it is needed to upgrade the software version, the old version may remain on the device. This feature enables the switch to start when the download of a new image version has failed and defected the internal FLASH . The boot procedure could be set to three modes of booting:

- **Primary**

  Starts the primary application that is saved on the first internal FLASH memory. If the application is missing or it is corrupt, the boot process stops and the device enters the Sysloader CLI.

- **Secondary**

  Starts the secondary application that is saved on the second internal FLASH memory. If the application is missing or it is corrupt, the boot process stops and the device enters the Sysloader CLI.

- **Auto**

  Starts first the primary application and if it fails the second application is activated. If both applications fail to start, the device enters the Sysloader CLI.

Images

Images that are provided to customers contain system loader and application image at the same time. When upgrading from a single boot version the image is downloaded as an ordinary image and after rebooting it upgrades the system to dual boot. After the upgrade only the primary image will persist. The upgrade procedure includes the Sysloader and the application using the same image.

SysLoader

When starting, the Sysloader counts down 5 seconds, allowing the user an entry point into the Sysloader's Command Line Interface (CLI). The Sysloader then passes to interactive mode, requests a login password, and starts a CLI session. If no key is pressed, the auto-startup of the switch application is performed.

While the switch reboots you will see numbers on the console terminal after the line “Press any key to stop auto-boot...”. To enter the Sysloader mode press any key while the numbers are running.

```
device_name#reload no-save
Proceed with reload ? [y/n] : y
Rebooting ...mu
```

```
Press any key to stop auto-boot...
 3




Nokia System Loader

Switch model            :  NOKIA ESB26
System Loader version   :  3.4.2 ER  Jan  8 2004 - 16:09:00
MAC address             :  00:A0:12:EE:01:47







User Access Verification

Password:
device_name>
```

Sysloader Commands

Application-Related Commands

The table below lists the switch Sysloader application-related commands.

Table APPENDIX-7 Application-Related Commands

Command	Description
start (primary|secondary) application	Terminates the Sysloader and starts execution of the application - primary or secondary.
download (primary|secondary) application	Copies the application from a source computer to the switch's permanent storage memory, through a console connection by X-modem transfer.
version	Displays the switch model type and the Sysloader version.
show boot-mode	Displays the configured boot mode (primary / secondary / auto)
swap application	Swaps the primary and secondary applications

Start Application

The **start application** command, in Sysloader mode, terminates the Sysloader and starts the execution of the chosen application.

Command Syntax

*device name>***start (primary|secondary) application**

Example

```
device_name>start primary application
```

```
Verifying validity of primary application.....OK


Start primary application...

BUILT-IN SELF TEST
------------------
CPU Core Test        : Passed
CPU Notify RAM Test  : Passed
CPU Interface Test   : Passed
Testing Switch Core  : Passed



////////////////////////////////////////////////////////////////////////
//                                                                    //
//                                                                    //
//       N O K I A                                                    //
//                                                                    //
//                                                                    //
//                                                                    //
//  Switch model : NOKIA ESB26                                        //
//                                                                    //
//  SW version   : 3.4.2 beta BG created Jan  8 2004 - 16:10:06       //
//                                                                    //
//                                                                    //
//                                                                    //
////////////////////////////////////////////////////////////////////////



User Access Verification

Password:
```

download application

The **download application** command, in Sysloader mode, copies the application from a source computer to the switch's permanent storage memory, through a console connection by X-modem transfer.

When you set the download command on the console, the switch waits for a file transfer.

The transfer starts in an X-modem format.

Upon completion of the transfer, the switch checks if the received file is a valid switch application code. If it is, the received image is stored in the internal FLASH memory.

This role of the **download application** command is to provide a rescue solution in case the switch becomes inoperable and there is no possibility to start either primary or secondary application.

Command Syntax

*device name>***download (primary|secondary|leave-primary-sw) application**

Argument Description

primary	Downloads the image to the first flash
secondary	Downloads the image to the secondary flash

leave-primary-sw	Moves the application from the first flash to second and stores a new image on it.

Example

```
device_name>download primary application
XMODEM application download to flash 0
XMODEM Receive: Waiting for Sender
Image Size = 0xBD552 CRC Value = 0x691181F3
Saving application code to FLASH bank 0....Success.
device_name>
```

swap application

The **swap application** command, in Sysloader mode, swaps the primary and secondary applications.

Command Syntax

```
device name>#swap application
```

show boot-mode

The **show boot-mode** command, in Sysloader mode, displays the configured boot mode.

Command Syntax

```
device name>#show boot-mode
```

Example

```
device_name>#show boot-mode
Boot mode is primary
```

version

The **version** command, in Sysloader mode, displays the switch model type and the Sysloader version.

Command Syntax

```
device name>version
```

Example

```
device_name>version



Nokia System Loader

Switch model           :  NOKIA ESB26
System Loader version  :  3.4.2 ER  Jan  8 2004 - 16:09:00
Primary version        :  3.4.2 ER
Secondary version      :  3.2.89 ER
MAC address            :  00:A0:12:EE:01:47

device_name>
```

Sysloader Configuration Commands

The table below lists the Sysloader configuration commands.

Table APPENDIX-8 Sysloader Configuration Commands

Command	Description
config	Switches from Loader mode to Loader Configuration mode.
mac-address	Displays or changes the switch's MAC address.
clean startup-configuration	Sets the startup configuration file to the factory default values.
clean java-image	Erases the Java image from the switch's memory storage.
clean boot-config	Clears the Sysloader EPROM.
clean log-history	Cleans all history records.
boot-mode	Sets the boot mode to primary, secondary or auto.
ip-address	Sets the outband IP address of sysloader (used for manufacturing only)

config

The **config** command, in Sysloader mode, switches the CLI from Sysloader mode to Sysloader Configuration mode.

The CLI prompt will change after executing this command.

Command Syntax

```
device name>config
```

mac-address

The **mac-address** command, in Sysloader Configuration mode, displays or changes the MAC address of the switch. If no argument is specified, the current MAC address is displayed.

Command Syntax

```
device name(config)#mac-address [HH:HH:HH:HH:HH:HH]
```

Argument Description

HH:HH:HH:HH:HH:HH	The switch MAC address.

Example 1

Displaying the switch's current MAC address:

```
device_name(config)#mac-address
Current base MAC Address of switch = 00:A0:12:1B:00:60
OutBand MAC Address (base + 1) = 00:A0:12:1B:00:61
```

Example 2

Assigning a new MAC address to the switch. The response indicates that the new MAC address is accepted and stored in the switch's memory.

```
device_name(config)#mac-address 00:a0:12:07:0f:78
New MAC Address of switch = 00:A0:12:07:0F:78
```

clean startup-configuration

The **clean startup-configuration** command, in Sysloader Configuration mode, erases the Startup configuration file saved in internal Flash memory.

Command Syntax

```
device name(config)#clean startup-configuration
```

clean java

The **clean java** command, in Sysloader Configuration mode, erases the Java image saved in internal Flash memory.

Command Syntax

```
device name(config)#clean java
```

clean boot-config

The **clean boot-config** command, in Sysloader Configuration mode, clears the Sysloader EEPROM.

NOTE Only Technical Support should use this command.

Command Syntax

```
device name(config)#clean boot-config
```

clean log-history

The **clean log-history** command, in Sysloader configuration mode, erases all the log history records.

For more information regarding the log history, see “Logging System Trap-Messages to the NVRAM**”**

Command Syntax

```
device name(config)#clean log-history
```

boot-mode

The **boot-mode** command, in Sysloader configuration mode, sets the boot mode to primary, secondary or auto.

By default, the boot mode is primary. For more information regarding the boot mode, see "Software Upgrade and Reboot Options"

Command Syntax

```
device name(config)# boot-mode (primary|secondary|auto)
```

Argument Description

primary	Boots the image from the first flash.
secondary	Boots the image from the secondary flash.
auto	Starts first the primary application and if it fails the second application is activated. If both applications fail to start, the device enters the Sysloader CLI.

Memory Debug Tools

The table below lists the commands for the memory debug tools.

NOTE Only the Technical Support should use the commands in this section.

Table APPENDIX-9 Sysloader Configuration Commands

Command	Description
memory	Switches from Sysloader mode to Sysloader Memory mode.
copy	Copies a block of memory.
display	Displays a block of memory.
fill	Fills a block of memory with a specified value.

memory

The **memory** command, in Loader mode, switches from Sysloader mode to Sysloader Memory mode.

The CLI prompt will change after executing this command.

Command Syntax

```
device name>memory
```

Example

```
device name>memory
device name(memory)#
```

copy

The **copy** command, in Sysloader Memory mode, copies a block of memory that is specified by block-length from the specified source address to the specified destination address.

Command Syntax

```
device name(memory)#copy <src-addr> <dst-addr> <blk-len>
```

Argument Description

src-addr	Hexadecimal source address (optionally prefixed with 0x).
dst-addr	Hexadecimal destination address (optionally prefixed with 0x).
blk-len	Hexadecimal or decimal block length (Use 0x prefix for hexadecimal number).

display

The **display** command, in Sysloader Memory mode, displays a block of memory, optionally specified by start address and block length in bytes.

Without any arguments, the command repeats the previous display, if any, or the default (after reload, the start address and block length are 0 and 256 respectively by default). If only the start address is specified, the previous or default block length is repeated.

Command Syntax

```
device name(memory)#display [<st-addr> [<blk-len>]]
```

Argument Description

st-addr	Hexadecimal start address (optionally prefixed with 0x).
blk-len	Hexadecimal or decimal block length (Use 0x prefix for hexadecimal number).

fill

The **fill** command, in Sysloader Memory mode, fills a block of memory by the specified hexadecimal value.

Command Syntax

```
device name(memory)#fill <st-addr> <blk-len> <value>
```

Argument Description

st-addr	Hexadecimal start address (optionally prefixed with 0x).
blk-len	Hexadecimal or decimal block length (Use 0x prefix for hexadecimal number).
value	Hexadecimal byte value to fill (optionally prefixed with 0x).