ES3000 Ethernet Switch

Advanced Concept Guide

symbol™
The Enterprise Mobility Company™

Advanced Concept Guide

72E-68445-01
Revision A
May 2004

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, New York 11742-1300
http://www.symbol.com

Contents

Chapter 3. Switch Management

Chapter 4. PoE Power Management

Chapter 5. Spanning Tree Protocols

Chapter 6. VLANs

Chapter 7. Link Aggregation

Chapter 8. QOS Management

Chapter 9. Port Security

Chapter 10. Port Mirroring

Chapter 11. Rate Limiting

Chapter 12. IGMP Snooping

Appendix A. Integrating with the Symbol WS 5000

Appendix B. Customer Support

Glossary

Index

Tell Us What You Think...

About This Guide

Introduction

The *Advanced Concept Guide* provides an introduction to the use of the ES3000 Ethernet Switch. This guide is aimed at network administrators who are experienced in configuring network devices or who want an introduction into some of the more advanced concepts involved in configuring Ethernet switches. For detailed instructions, please see the *ES3000 Users Guide*.

Notational Conventions

The following conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Service Information

If a problem with is encountered with the equipment, contact the Symbol Support Center for your region. Please see *Appendix B, Customer Support* for customer support contact information. Before calling, have the model number and serial number at hand.

Call the Support Center from a phone near your network equipment so that the service person can try to talk you through your problem. If the equipment is found to be working properly and the problem is symbol readability, the Support Center will request samples of your bar codes for analysis at our plant.

If the problem cannot be solved over the phone, you may need to return your equipment for servicing. If that is necessary, you will be given specific directions.

Symbol Technologies is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty. If the original shipping container was not kept, contact Symbol to have another sent to you.

For the latest version of this guide go to: http://www.symbol.com/manuals.

1

ES3000 Hardware Notes

1.1 Hardware Notes

The ES3000 Layer 2 Ethernet switch comes in two versions. One version provides power over Ethernet (PoE) in accordance with IEEE standard 802.3af. This allows compatible Ethernet devices to obtain power from the 10/100BaseT Ethernet wiring. The details of the PoE implementation are described in *Chapter 4, PoE Power Management*. IEEE 802.3af PoE senses the need for power before supplying power and will not damage non-PoE Ethernet devices.

The other version of the ES3000 switch does not provide power over Ethernet. The power features described in *Chapter 4, PoE Power Management* are not available in the non-PoE version of the switch.

The PoE and non-PoE versions of the ES3000 switch use different versions of the bootcode and runtime software. Do not attempt to use PoE software with a non-PoE switch. Do not attempt to use non-PoE software with a PoE switch. Attempting to do so may render the switch inoperable.

2

ES3000 Software Management

2.1 Initial Communication with the Switch

The ES3000 Layer 2 Ethernet switch uses three means of communication for administration of the switch: serial communication via the DB-9 cable on the front of the system, telnet communication over the network, and http communication over the network. Almost all configuration can be done using any of these means of communication. However, bootcode reconfiguration requires that the administrator be using serial communication.

The only purpose of the IP address for the switch is to facilitate communication with the switch. The ES3000 switch defaults to DHCP for its IP address. If an installation requires that the switch have a fixed IP address, the IP address should be set using the serial interface.

The serial communication parameters of the ES3000 switch are 19200 baud, 8 bits, no parity, one stop bit, hardware flow control, and VT100 emulation. The ES3000 has a male DB-9 connector.

2.2 Setting The Switch IP Address

To set the IP address using the serial communication system, allow the ES3000 to boot. After some self-test messages, the ES3000 will display a login prompt:

```
==================================================
ES3000-PWR Local Management System
Symbol Technologies, Inc.
Copyright, 2004
==================================================
Login Menu

Login:
```

Log in as the *admin* user. The default password for the admin user is “symbol”.

The main menu will display:

```
Main Menu

[G]eneral Info.
System [A]dmin. ...
[P]orts ...
[V]LANs ...
[I]GMP Snooping ...
```

```
Spanning [T]ree ...
Qo[S] ...
[E]xecute CLI
[Q]uit

Command>
```

Select "A" for "System Admin", then "A" for "Access" and "I" for "IP Config."

The following screen will display:

```
Access -> System IP Configuration Menu

MAC Address:        00:30:AB:25:81:31
IP Address:         192.168.2.50
Subnet Mask:        255.255.255.0
Default Gateway:    192.168.2.1
DHCP Mode:          Disabled

--------------------------- <COMMAND> -----------------------------
Set [I]P Address
Set Subnet [M]ask
Set Default [G]ateway
Set [D]HCP Status
Set DHCP [R]enew

[Q]uit to previous menu
```

Disable DHCP, and set the IP address, subnet mask, and default gateway. Communication using the specified IP address should now be possible.

Unless the switch configuration is saved, the IP address will remain functional only until the switch reboots. To save the switch configuration, quit out to the main menu, enter "A" for "System Admin.","T" for "Tools", and "S" for "Save Config". The switch will save the IP address along with other configuration parameters in flash memory.

2.3 Bootcode and Bootcode Prompt

The software on the ES3000 switch is in two parts: the bootcode and the runtime code. The bootcode can only be updated through the serial interface to the switch.

The steps to upgrade the bootcode are

1. Make the bootcode available on a TFTP server.
2. Establish serial communication with the switch.
3. Power-cycle the switch and interrupt the self-test phase.
4. Download the bootcode file.
5. Install the bootcode.

2.3.1 Make the Bootcode Available

Symbol Technologies will make bootcode upgrades available through the Symbol support pages on the web and, if needed, through other means of distribution. The PoE version of the ES3000 and the non-PoE version of the ES3000 require, at this time, different versions of the bootcode.

Do not attempt to run PoE versions of the bootcode on non-PoE versions of the switch or vice versa or the switch may not be operable after the incorrect bootcode is installed.

After the bootcode is downloaded from Symbol Technologies, place the bootcode in the service directory for any TFTP server on the same LAN as the ES3000 switch. There are many TFTP servers available, some at no cost. The procedures in this section were tested using the Solar Winds TFTP server for Windows, available at www.solarwinds.net.

2.3.2 Establish Serial Communication with the Switch

If needed, establish serial communication with the ES3000 switch. As stated above, the serial communication is through a male DB9 connector on the front of the ES3000. The communication parameters are 19200 baud, 8 data bits, no parity, one stop bit, hardware flow control.

2.3.3 Power-Cycle the Switch and Interrupt Self-Test

The bootcode upgrade can not be installed from the normal level of software on the ES3000. To install new bootcode, power-cycle the switch. It will print out messages as it boots:

```
Booting...

Memory test......OK
```

```
System database initialization ... OK
PCI unit 0: Dev 0x5645, Rev 0x11, Chip BCM5645_B0, Driver BCM5615_A0
Attaching SOC unit 0... PCI device BCM5645_B0 attached as unit 0.


BCM register test ............ PASS
PHY register test ............ PASS
Internal MAC loopback test ... PASS


Checking Image Bank Integrity ...  OK
```

While the switch is booting, type one or more control-c characters.

The switch should enter the boot system interface:

```
StrataSwitch II Series Boot System

Version 1.0.0.0-012R / Apr 26 2004 11:44:48

>>> Main Menu <<<

TCP/[I]P Configuration
[S]oftware Upgrade
[J]ump to Runtime Code

Command>
```

Enter “S” for “Software Upgrade”.

2.3.4 Download the Bootcode File

The ES3000 will display the following:

```
StrataSwitch II Series Boot System

Version 1.0.0.0-012R / Apr 26 2004 11:44:48

Remote Server IP: 192.168.2.39
Remote File Name: ES3000_PWR_run_1-0-0-0-909R.rom
```

```
>>> Software Upgrade Menu <<<

Set Remote [S]erver IP Address
Set Remote [F]ile Name
[D]ownload software and Execute
Download [B]ootcode and Execute
Download [P]oL controller image
[Q]uit to Previous Menu

Command>
```

Enter "S" for "Set Remote Server IP Address" and enter the IP address of the TFTP server. Enter "F" for "Set Remote File Name" and then the name of the bootcode file. Finally, enter "B" for "Download Bootcode and Execute." The bootcode will download and as it does the switch will show the number of bytes received from the TFTP server.

2.3.5 Install the Bootcode

After the bootcode has been downloaded to the switch, the following screen will display:

```
Bytes received :  780194

Downloading file was completed!

Checking Image file integrity ... OK

Version:     1.0.0.0-012R
Date Time:   Apr 26 2004 11:44:48

Do you want to update boot image? [Y/N]
```

To install the bootcode, answer "Y" and press "Enter". The system will then make a boot image of the new bootcode and then reboot the switch:

```
Updating the boot image ... OK

Booting...
```

The bootcode for the switch has been updated.

2.4 Runtime Software

The runtime software for the switch can be installed from the serial interface, the telnet interface, or the web interface. From the serial interface or the telnet interface, the installation procedure is the same.

1. Make the runtime software available on a TFTP server.
2. Download the runtime software file.

2.4.1 Make the Runtime Software Available on a TFTP server

Symbol Technologies will make runtime software upgrades available through the Symbol support pages on the web and, if needed, through other means of distribution. The PoE version of the ES3000 and the non-PoE version of the ES3000 require, at this time, different versions of the runtime software.

Do not attempt to run PoE versions of the runtime software on non-PoE versions of the switch or vice versa or the switch may not be operable after the incorrect runtime is installed.

After the runtime software is downloaded from Symbol Technologies, place the runtime software in the service directory for any TFTP server on the same LAN as the ES3000 switch. There are many TFTP servers available, some at no cost. The procedures in this section were tested using the Solar Winds TFTP server for Windows, available at www.solarwinds.net.

2.4.2 Download the Runtime Software

To download the runtime software to the switch, using the menu interface, select “A” for System Administration, “T” for Tools and “U” for Software Upgrade. The Software Upgrade screen will display:

```
Tools -> Firmware Upgrade

Image Version/Date:   v1.0.0.0-909R / Apr 29 2004 17:25:09
TFTP Server IP:       0.0.0.0
Image File Name:|
---------------------------- <COMMAND> --------------------------------
```

```
Set TFTP [S]erver IP Address
Set Image [F]ile Name
[U]pgrade Image
[Q]uit to previous menu


Command>
```

Enter "S" to set the server IP number to the IP number for the TFTP server. Enter "F" to set the runtime software filename. Enter "U" to install the new runtime software image. The runtime software will download and install and the switch will reboot. This process may take several minutes to complete.

2.5 Resetting the Switch

If the password to the switch if lost or forgotten, the switch may be reset to the factory defaults, including the default password of "symbol" by the following:

1. Establish serial communication with the switch
2. Power cycle the switch
3. During the boot cycle repeatedly enter Escape (esc) characters
4. When the system asks "`Reset configuration to factory default (y/n)?`" answer with "Y"

During this procedure, the screen in communication with the switch will look like:

```
Memory test......OK
System database initialization ... OK
PCI unit 0: Dev 0x5645, Rev 0x11, Chip BCM5645_B0, Driver BCM5615_A0
Attaching SOC unit 0... PCI device BCM5645_B0 attached as unit 0.

BCM register test ............. PASS
PHY register test ............. PASS
Internal MAC loopback test ... PASS

Checking Image Bank Integrity ...  OK

Booting system ...

Decompressing...OK

Press 'ESC' key to reset to factory default ...
```

```
Attaching SOC unit 0...
GBP auto-sized to 16 MB, 4 banks, 64-bit bus
MMU initialized.
BCM driver initialized.
ARL DMA shadowing enabled.
Port modes initialized.

MSR Task creation is successful
CLI Task creation is successful

Reset configuration to factory default ? ( y/n )
```

Afterwards, the system will reboot and will be available with the default passwords. The system will *not* be configured. The configuration information is removed to prevent confidential information from falling into the hands of someone who does not know the password but who does not the reset procedure.

3

Switch Management

3.1 Managing the Switch

This chapter describes the following switch management functions:

- Configuring Simple Network Management Protocol (SNMP)
- Viewing port counters
- Saving configuration changes
- Updating the switch software
- Rebooting the switch

3.2 SNMP

3.2.1 Overview

Simple Network Management Protocol (SNMP) is a messaging protocol that allows communication between network managers and agents. An SNMP manager is part of a network management system (NMS), and allows the administrator to manage the network by making requests to agents. An SNMP agent provides an interface to a managed device, which contains managed objects in a management information base (MIB).

At the request of an SNMP manager, an SNMP agent retrieves or stores values in the device described in the MIB. The SNMP agent can also send asynchronous traps, which alert the SNMP manager to certain conditions on the network. A trap might result from improper user authentication, PoE power usage over threshold, or network topology changes, for example.

In the ES3000 switch, the agent and the MIB reside on the switch. To configure SNMP on the switch, the administrator sets up the relationship between the agent and the SNMP managers.

The ES3000 switch supports the following standard MIBs:

BRIDGE-MIB	RADIUS-AUTH-CLIENT-MIB
IEEE8021-PAE-MIB	RADIUS-ACC-CLIENT-MIB
IEEE8023-LAG-MIB	RFC123-MIB
IF-MIB	RMON-MIB
IP-MIB	SNMPv2-MIB
P-BRIDGE-MIB	TCP-MIB

POWER-ETHERNET-MIB UDP-MIB

Q-BRIDGE-MIB

The ES3000 switch also supports the *Symbol-ES3000-MIB-06a* MIB. This Symbol Technology proprietary MIB allows SNMP to be used to initiate the TFTP download of runtime firmware to the ES3000 switch and to initiate the uploading or downloading of ES3000 configuration files.

3.2.2 Configuring SNMP Communication

To configure SNMP, the administrator sets up

- General system information
- A list of managers allowed to access the agent's MIB information
- A list of managers that receive traps

3.2.2.1 System Information

Use the System Information page (*System Admin. > SNMP Config. > System info.*) to set the switch agent's name, contact, and location information. This page displays the following:

- **System Description:** A description of the switch.
- **System Object ID:** The MAC address of the switch.
- **System Name:** The switch identification. The value can be a string up to 50 characters long.
- **System Location:** The switch location. For example, "Building M, Room 205." The value can be a string up to 50 characters long.
- **System Contact:** Contact information for the switch. For example, "Contact Switch System Admin at x62304." The value can be a string up to 50 characters long.

3.2.2.2 Manager Authorization

Use the Manager Authorization page (*System Admin. > SNMP Config. > Authorized Managers)* to define the relationship between SNMP managers and the agent, which enables authorized SNMP managers to access the MIBs on the switch. The administrator can also prevent unauthorized access.

The relationship between managers and agents is defined through a community string, which functions like a password, and is associated with privilege, either read-only or read-write. The administrator can also restrict communities to specific IP addresses.

This page displays a table of SNMP manager communities. The administrator can set or change the parameters for each one. To apply the changes, click Apply. The page displays the following:

- **Status:** Enables or disables SNMP access for the community. The administrator can set the status to Enabled to allow access or Disabled to prevent access.
- **Privilege:** An access privilege associated with the community/IP address pair. The administrator can select either Read-Only or Read-Write. The default for Privilege strings is Read-Only.
- **IP address:** An optional IP address that additionally restricts a community to a specific IP address. If the administrator leaves this field at 0.0.0.0, the switch authorizes SNMP managers at all IP addresses, provided they supply the community string.
- **Community:** A community name. This functions as a password. The administrator must enter a value to enable manager authorization. The switch has two communities enabled by default: private, with read-write access for all IP addresses, and public, with read-only access for all IP addresses. The value is a string up to 20 characters in length.

3.2.2.3 Trap Receivers

Use the Trap Receiver page (*System Admin. > SNMP Config. > Trap Receivers)* to enter the SNMP managers that receive SNMP traps, which alerts the SNMP manager to specific conditions on the network. To apply the changes, click Apply. The page displays the following parameters for each manager:

- **Status:** Enables or disables trap reception for the community. The administrator can set the status to Enabled to allow trap reception, or Disabled to prevent trap reception.
- **Type**: The SNMP MIB version. Set to v1 for SNMPv1 MIB or to v2 for SNMPv2 MIB.
- **IP address:** The IP address of the manager that receive the traps. To enable trap reception, the administrator must enter a specific IP address.
- **Community:** A community name. This functions as a password. The administrator must enter a value before a trap reception is enabled. The value is a string up to 20 characters in length.

3.2.3 Configuring SNMP Traps

Use the Trap Selection page (*System Admin. > SNMP Config. > Trap Selection*) to choose which events generate SNMP traps. The switch generates traps only when a trap receiver exists. The administrator can enable or disable the following traps:

- **SNMP Cold Start:** Generates a trap when the switch is rebooted.
- **SNMP Authorization Failure:** Generates a trap when a host attempts to access the switch whose IP address is not in the Manager Authorization table.

- **Bridge Topology Change:** Generates a trap if switch-to-switch connections change.
- **Bridge New Root:** Generates a trap if a topology change results in a new root switch.
- **RMON Alarm Trap:** Generates a trap when a remote monitoring (RMON) alarm is triggered.
- **Config Change:** Generates a trap for SNMP configuration changes.
- **SNMP ACL Violation:** Generates a trap when SNMP communication is attempted from an IP address which is not listed as a possible IP source, without regard as to whether the correct community strings were offered.
- **PoE Trap Control:** Generates a trap when PoE has exceeded threshold power capacity.
- **Enabled Link Up/Down Control:** The administrator enters the port numbers for which to enable link control. When a port is listed, the switch generates a trap when the port link goes down or up. Enter a comma-separated list of port numbers. For example: 2,4,5-12.

3.3 Port Counters

Use the Port Counters page (*System Admin. > Ports > Port Counters)* to view traffic information for each port. The switch tracks information about the following counters:

Total RX Bytes	Oversize Packets	128-255 Packets
Total RX Packets	Fragments	256-511 Packets
Good Broadcast	Jabbers	512-1023 Packets
Good Multicast	Collisions	1024-1518 Packets
CRC/Align Errors	64-Byte Packets	
Undersize Packets	65-127 Packets	

The Port Counter page initially displays counter information for port one, and the counters reflect the values since the system was last booted or powered on. To refresh the counters, click the Refresh Now button.

The administrator can reset the counter values for this port to 0 by clicking Reset. Then the administrator can choose whether to view the counters since power-on or reboot, or since the reset, by clicking on either the Since System Up or Since Reset buttons. If the administrator navigates out of the Port Counter page, the switch does not maintain the reset time.

To display counter information for a specific port, enter the port number and click Apply. To compare counter values across ports for a specific counter, click on the name of the counter. The switch then

displays a page with that counter's value shown for all ports. The administrator can use the Refresh Now button to refresh the page for updated information.

3.4 Configuration Files

After the administrator has modified the switch configuration to meet the needs of the network, he can save the configuration either to flash memory or to a configuration file. The switch will not respond to ping requests during the configuration save.

The administrator can upload configuration files to a Trivial File Transfer Protocol (TFTP) server and download them to the switch at a later time.

The contents of the configuration file will be a list of CLI commands, sufficient to take the switch from the factory default state to the current state of the switch. When downloading a configuration file to a switch, the switch will execute each of the CLI commands. If the configuration file is downloaded to a switch which has been reset to the defaults before the download, the result will be a duplicate of the original switch configuration. If the configuration is downloaded to a switch with an existing configuration in place, the downloaded configuration will be overlaid over the existing configuration and the result may not be a duplicate of the original switch configuration.

If a large number of ES3000 switches must be configured, it may be worthwhile to manually configure one switch, examine the resulting configuration file, and use a scripting language to modify the switch to create near duplicates for configuration of the other switches.

3.4.1 Saving Configuration to Flash Memory

Use the Save Configuration page (*System Admin. > Tools > Save Config*) to save configuration changes to flash memory, which allows the configuration to endure power cycling and rebooting of the switch. Click the Save Configuration button.

3.4.2 Downloading/Uploading Configuration Files

Use the TFTP Configuration File Upload/Download page (*System Admin. > Tools > Upload/Download Config*) to save the configuration in a configuration file, and later restore the configuration from this file.

Saving and restoring configurations requires a TFTP server. The switch has been tested with the Solar Winds TFTP server freeware that is available for download at www.solarwinds.net.

Save the current configuration to a file to a TFTP server by entering the TFTP server IP number and a configuration file name, and then clicking on the Upload button.

Retrieve a configuration from a file from a TFTP server by entering the TFTP server IP number and a configuration file name, and then clicking on the Download button.

3.5 Software Updates

Symbol periodically releases new versions of the software that runs on the switch. These software releases provide new features and functionality. To upgrade the switch to incorporate these changes, use the Software Upgrade page (*System Admin. > Tools > Software Upgrade)*.

Enter the IP address of the TFTP file server where upgrades are located, and the name of the software image file. Click Apply to upgrade the software in the switch.

The software upgrade overwrites the previous version of the runtime image in the switch.

3.6 Rebooting the Switch

To reboot the switch, use the System Reboot page (*System Admin. > Tools > System Reboot)*. The switch provides three reboot options:

- **Normal:** Upon reboot, the switch returns to the configuration saved in Flash memory.
- **Factory Default:** Upon reboot, the system returns to the factory default configuration.
- **Factory Default Except IP:** Upon reboot, the system returns to the factory default configuration, but retains the IP address assigned for this network.

Click Apply to reboot the switch.

3.7 Using DHCP to Load Configurations

Although DHCP service is used primarily to set IP addresses, netmasks, and default gateways for DHCP clients, the DHCP standard also provides for vendor defined options to be downloaded to the DHCP clients. The ES3000 can make use of this capability.

The ES3000 switch recognizes the following DHCP options:

- 183: TFTP server IP address
- 185: Runtime software filename on the TFTP server
- 186: Configuration filename on the TFTP server

If options 183 and 185 are set, the ES3000 will compare the runtime software filename with the filename of the runtime software in use. If the filenames are different, the switch will download the file identified by the filename in the DHCP information, load it, and reboot.

If options 183 and 186 are set, ES3000 will download and use the configuration file specified in the DHCP information.

If options 183, 185, and 186 are set, the ES3000 will download the runtime software and reboot before downloading and using the configuration file.

4

PoE Power Management

4.1 Power over Ethernet (PoE) Overview

4.1.1 PoE Terms and Standards

Power over Ethernet (PoE) supplies power to Ethernet devices directly through the Ethernet data cable. PoE distinguishes between two types of equipment: power-supply equipment (PSE), such as the ES3000 switch, and a powered device (PD), such as an access point. If the powered device requires power, the PSE injects the current into the cable, and the powered device can operate solely through the power it receives from the data cable.

The standard for PoE is IEEE 802.3af. The ES3000 switch is compliant with this standard.

4.1.2 PoE Sensing

ES3000 switch can sense whether a powered device is attached to a port. The switch supplies power only to devices that need it. The switch initially uses resistance detection (802.3af) to determine whether a port requires power. If that fails, and if capacitance detection is enabled, the switch then uses capacitance detection to determine whether the port needs power. This allows the switch to detect the presence of legacy powered devices, which might not be 802.3af compliant.

4.2 Power Management

4.2.1 Power Management Overview

The ES3000 switch has a maximum PoE power budget of 170 watts. This is enough to supply 7 watts to all 24 PoE ports on the switch. The switch supplies a maximum of 16.5 watts per port.

When a new powered device is connected to a port, the ES3000 switch checks whether enough power remains in the power budget to support the device. This decision is based on the actual power drawn by the powered devices at the time of connection, rather than their maximum power consumption. Each powered device will usually draw less power than it maximum limit.

If there is insufficient power to supply all PoE-enabled ports, the switch does not power all ports. The administrator can select the method the ES3000 switch uses to decide which ports receive power; see “Configuring the Switch Policy” on page 4.

The web interface has two configuration pages. The PoE Port Configuration page allows the administrator to manage and monitor power restrictions for individual ports. The PoE Global Configuration page allows the administrator to set PoE management policies that affect the entire switch.

4.2.2 Configuring and Monitoring Ports

Use the PoE Port Configuration page. (*Ports > Power Over Ethernet > PoE Port Config.*) to configure and monitor the PoE status for each port. The Port Configuration page displays the following:

- **Port:** The physical port number.
- **PoE:** Enables or disables power to the port. Set the Admin parameter to either On or Off. On or Up means that the switch may supply power to the port, Off or Down means that the switch will not supply power to the port under any circumstance. If PoE is On, the display shows Up. If PoE is Off, the display shows Down. The default is Up.
- **Status:** The port's power status. When a powered device is connected and enabled and the ES3000 is currently providing power, Powered is displayed. Otherwise, Not Powered is displayed.
- **Class:** The powered device's classification. The powered device can inform the switch of its maximum power consumption, called its classification. If the device has a classification, it automatically informs the switch, which displays the information. The switch does not use classification for any decision-making processes. However, the administrator can use this information to set the power limit for a port using the Limit parameter. The display will show "---" for a port which has no powered devices connected to it. If there is a PD connected to the port, the default is class 0, or an unclassified PD. If the PD gives its classification, then that classification is displayed. All Symbol Technology PoE Access Ports are currently unclassified.

Class	Usage	PSE Output Max Power (Watts)	PD Power (Watts)
---	Not a PoE device		
0	Unclassified POE device	15.4	0.44-12.95
1	Optional	4	044 - 3.84
2	Optional	7	3.84 - 6.49
3	Optional	15.4	6.49 - 12.95

- **Priority:** The priority of a port. This value is only used when the power management method is priority-based. See "Configuring the Switch Policy" on page 4. The Priority parameter can be set to Critical, High, or Low. When two ports have the same priority level, the lower numbered port has the higher priority. For example, if both ports 8 and 15 are set to High priority, port 8 has higher priority than port 15. The default is Low.

- **Limit (W):** The maximum power the switch will supply to the port. The Limit parameter can be set within the range of 3W to 16.5W. Under the web interface, the menu used to set the power limit shows the Symbol recommended power limits for Symbol Access Ports.
  Do not set this value based on the Power display. This displays power currently provided to the device. The powered devices power requirements can fluctuate above or below the level currently displayed in the Power parameter, and service will be dropped if power requirements exceed the limit for the port. The default is 16.5W.
- **Power (W):** The power currently provided to the device in watts.
- **Voltage (V):** The voltage currently provided to the device in volts.
- **Current (A):** The current currently provided to the device in amps.

4.2.2.1 Symbol Access Port PoE Limits

The following table shows the Symbol recommended power limits for some typical Symbol Access Port configurations.

Access Ports	Recommended Power Limit
AP 100	4.5 w
S24 AP with Power Converter	8.5 w
AP 200 / 802.11a only	9.0 w
AP 200 / 802.11a & b	11.0 w
AP 200/802.11a and AP100	14.5 w
AP 200/802.11a&b and AP100	16.5 w

Under normal operating conditions, actual power use may be less than half of the recommended limit. The margin is important to allow for rises in power use from high bandwidth usage, exceptional operating conditions, and manufacturing variation. A reasonable guess for the power limit for a non-Symbol powered device is twice the actual power draw under typical conditions.

4.2.3 Configuring the Switch Policy

Use the PoE Global Configuration page (*Ports > Power Over Ethernet > PoE Global Config.*) to set policy decisions that apply to the switch as a whole, including powered device detection method, power management method, and power usage threshold.

Changes made to this screen will not take effect until the administrator clicks the Apply button. The PoE Global Configuration page displays the following parameters:

- **Power Budget:** Maximum total power available for all PoE ports. The switch has a power budget of 170 watts. This value cannot be changed.
- **Detection Method:** Enables or disables the capacitance detection method to determine whether a powered device requires power. This parameter applies only to older powered devices. If capacitance detection is enabled, the switch applies capacitance detection to determine whether the device requires power. Older devices might not be recognized by the switch when capacitance detection is disabled. The switch detects newer powered devices regardless of the setting of this parameter. The default is Capacitor Detection Disabled.
- **Power Management Method:** Sets the method the switch uses to determine which ports receive power when the power budget is exceeded. Two methods are available:
  - Deny next port connection, regardless of priority: The switch continues providing power to previously connected and enabled powered devices, and denies the request of a newly connected or enabled powered device. This is the default setting.
  - Low-priority port will be shut down: The switch searches previously connected powered devices for one with a lower priority than the new powered device. The switch discontinues power to the lower-priority device and gives preference to the higher-priority device. If the power budget is still exceeded after discontinuing power to the lower-priority device, the algorithm loops to find the next lowest-priority port to shut down.
- **Power Usage Threshold:** The threshold at which to enable a SNMP trap to warn an SNMP trap receiver that power usage is above a threshold level. This is a warning only, and does not affect power supplied to the ports. The administrator can set this value as a percentage of the total power budget. When the total power provided by the switch to all ports exceeds this percentage of the power budget, an SNMP trap is sent. The trap is only sent if an SNMP trap receiver has been set up. The default value is 80%.

4.2.4 Symbol Recommendations for Power Policy

Symbol believes that most installations will be optimally served by the following power policy:

- Set the power limit for the powered devices to the limits recommended in *Symbol Access Port PoE Limits on page 4-4*.
- Do not let the total of all power limits exceed the 170 watt power budget.
- Set power priority of ports with PoE devices on them to critical or high.

- Use priority-based power management.
- Either set the priority of currently unused ports to low and set the power budget for these ports to 16.5 watts.

Under this policy, low-priority ports will be available as unmanaged powered ports. If there comes a time when there is insufficient power to supply all ports, the high-priority, managed, ports will receive power and some or all of the low-priority ports will not. If a powered device, either high or low priority, malfunctions and draws more than its power limit, the power to that port will be shut down until the power draw is beneath the established limit.

4.2.5 Troubleshooting

4.2.5.1 Existing PD loses power when new PD connected.

If power on an existing port shuts down when a new powered device is connected, the switch is probably using a priority-based system for determining which ports receive power. If the switch has exceeded its power budget, and if the new powered device has a higher priority than the existing device, the switch shuts down the existing device.

4.2.5.2 Newly connected powered device not receiving power.

Several situations can cause a newly connected powered device to not receive power from the switch:

- Power is disabled for the port. Check on the PoE port configuration page, and ensure that the port for this device is Up.
- The switch has exceeded its power budget, and "Deny next port connection" is in effect on the PoE Global Configuration page.
- If the powered device is an older device, it might not be detected as requiring power unless "Capacitor Detection Enabled" is set on the PoE Global Configuration page.

5

Spanning Tree Protocols

5.1 Spanning Tree Overview

The ES2000 switch can be configured to use one of three spanning tree protocols. Spanning Tree Protocol (STP) is compatible with legacy equipment. Rapid Spanning Tree Protocol (RSTP) is significantly faster than STP. Multiple Spanning Tree Protocol (MSTP) is based on RSTP and extends RSTP in a way that is useful for switches implementing VLANs.

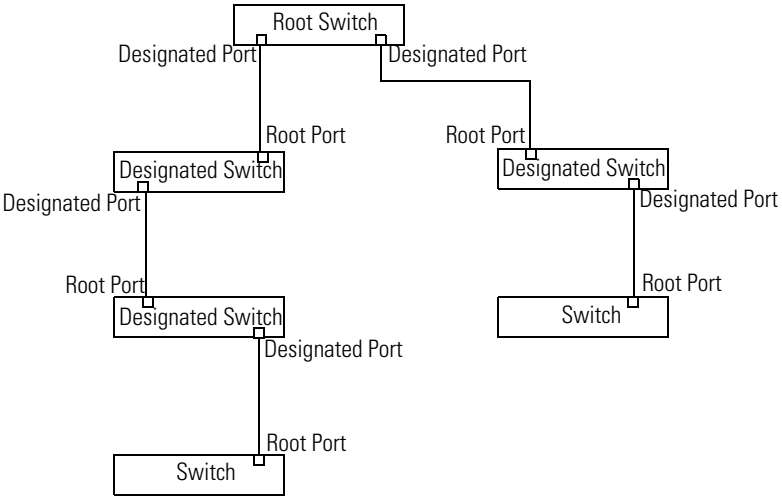
5.2 Spanning Tree Protocol (IEEE 802.1D)

The Spanning Tree Protocol (STP) ensures that no loops are formed in a meshed network while providing a path between any two nodes in the network. STP finds non-looping paths between stations by requiring switches to exchange messages called bridge protocol data units (BPDU). BPDUs contain information about the switch and its connections to other switches.

For each VLAN, the STP process selects a root switch. If the switches differ in priority, the root switch is the switch with the highest priority. If all switches are of equal priority, the root switch is the switch with the lowest MAC address. It is usually best for the root switch to be the switch which has the fastest connection to the outside world. The network administrator can force this switch to be the root switch by assigning it the highest priority (lowest numerical value).

After a root switch has been chosen, a single path is chosen from that switch to all other switches, disabling or blocking the other paths. If there are multiple paths to another switch, it will first choose the path to the highest-priority switch. If all switches have the same priority, it will choose the path with the lowest cost. If all paths have the same cost, it will choose the path to the lowest MAC address.

The port which connects a non-root switch to the root switch, directly or indirectly, is known the *root port* for that switch. A switch which is used as the connection between the root switch and another switch is known as the *designated switch* for the destination switch. The port on a designated switch which is selected for communication with a non-root switch is known as the *designated port* for the destination switch.



5.3 Configuring STP

MSTP is much faster than STP. STP is only at an advantage if there is legacy equipment in the network topology that does know how negotiate an MSTP cycle. If that is the case, then all of the network equipment in the local network must use STP. To configure STP:

1. Set the switch priority and timing parameters.
2. Refine the port path costs, if needed.

5.3.1 Set Switch Priority and Timing Parameters

The STP configuration parameters are set using the CIST Configuration page.

1. Use the left menu to navigate to the CIST Configuration page (*Spanning Tree > MSTP Config. > CIST Config.*).
2. If there is a switch that is closest to the WAN and therefore should be the favored root switch, set the CIST Bridge Priority on that switch to a lower number (higher priority).

Usually, it will not be necessary to change the timing parameters for an STP switch. If desired, these can also be set on this page. See *Set the Configuration Timing Parameters on page 5-6* for an explanation of the timing parameters.

3. Click on the Apply button at the bottom of the web page to record the changes.

5.3.2 Refine Port Parameters

When choosing a path from one switch to another, the spanning algorithm will:

- Choose the port marked with the highest priority (lowest number)
- If there is more than one port with the (same) highest priority, choose the port with the lowest cost
- If there is more than one port with the lowest cost, choose the port with the lowest MAC number

By default, all ports will have the same priority. By default 10BaseT links have a cost of 2000000, 100BaseT links have a cost of 200000 and Gigabit links have a cost of 20000.

If desired, the port priority and cost parameters can be tuned on the CIST Basic Port Config. page (*Spanning Tree > MSTP Config. > CIST Basic Port Config*). The other parameters on this page have no effect on STP spanning trees. They are used in MSTP spanning trees.

5.4 Rapid Spanning Tree Protocol (IEEE 802.1W)

STP has the disadvantage that it can take a long time, up to fifty seconds, to select a root switch and to prune the set of all links to a non-looping tree. Under STP, this selection of a root switch and pruning to a non-looping tree must be duplicated every time a change is made to the network topology. Since traffic is not forwarded during the reconfiguration, this can lead to unacceptable interruptions in service. Rapid Spanning Tree Protocol (RSTP) can trim the reconfiguration time to a second or less.

RSTP acquires and stores more detailed information on the network topology. When the topology changes, RSTP reconfigures the spanning tree incrementally rather than building the entire spanning tree from scratch. The combination of the two results in a much faster reconfiguration time.

For example, besides classifying ports as root ports and designated ports, RSTP also classifies ports as alternate ports and backup ports. Alternate ports provide alternate links to the root switch than the current root port in use. Backup ports provide a backup link to the destination switches other than the designated port currently in use. When a given path from the root switch toward the leaves of the spanning tree fails, RSTP provides that the switch still connected to root propose use of the alternate port to the switch on the other side of the that port. If that switch accepts, the spanning tree change is made and forwarding resumes.

RSTP also distinguishes edge ports and point-to-point link ports. Edge ports are ports that connect to a single end station. Edge ports do not take part in spanning tree reconfiguration, enabling faster

reconfiguration. Point-to-point link ports are ports that connect to another switch. Point-to-point links are reconfigured with a proposal-agreement dialog that is much faster than rebuilding the entire spanning tree.

If an RSTP-enabled switch is connected to a switch that cannot communicate using RSTP BPDUs, the RSTP-enabled switch will communicate with the legacy switch using STP BPDUs. The spanning tree will still reconfigure successfully, but it will do so much more slowly than it would if only RSTP-enabled switches were connected. If possible, make sure that all the switches in a spanning-tree domain are of one type or another, not a mix.

5.4.1 Multiple Spanning Tree Protocol (IEEE 802.1S)

Multiple Spanning Tree Protocol (MSTP) allows the creation of multiple spanning tree domains. Each spanning tree instance provides the same advantages as the regular Spanning tree - however now the network administrator can utilize the links in the network to their fullest. Load balancing spreads the traffic across the multiple paths, improving performance. MSTP also deals properly with VLANS that cross switch boundaries. MSTP is compatible with RSTP. MSTP uses a modified RSTP for rapid convergence of spanning tree data.

MSTP spanning trees are also called MSTP instances. MSTP instances are grouped together into MSTP configurations, also known as MSTP regions.

Each MSTP configuration consists of one or more MSTP instances. An MSTP configuration has a number, a name, and a revision level. The MSTP instances within an MSTP configuration must share protocol timing values - Hello Time, Maximum Age, and Forward Delay. A given switch may only be part of one MSTP configuration.

Each MSTP instance is a spanning tree, but its members are VLANs rather than switches. The MSTP instance may have one or more VLANs. A given VLAN may only participate in one MSTP instance.

Each MSTP configuration will have an instance root and the instance root will store the internal spanning tree (IST) for the MSTP configuration. The MSTP configurations will communicate and establish a common spanning tree (CST) which maps forwarding path information between the different MSTP configurations. The combination of the common spanning tree and internal spanning trees is called the common and internal spanning tree or CIST.

5.5 Configuring MSTP and CIST

The process of configuring a switch for MSTP consists of the following steps:

1. Enable and define an MSTP configuration.
2. Set the timing parameters for the configuration.
3. If desired, define special tuning characteristics for the ports in the switch.
4. Assign the VLANS on the switch to individual MSTP instances.

5.5.1 Enable and Define MSTP Configuration

1. Use the left menu to navigate to the Multiple Spanning Tree Configuration page (*Spanning Tree > MSTP Config. > MSTP Config.*).
2. Set the Global MSTP Status to *Enabled* and press the Apply button to the right.
3. Set the Protocol Version to *MSTP* and press the Apply button to the right.
4. Set the MSTP Config ID Selection to a number between 1 and 255.
5. Set the MSTP Configuration Name to a string, 32 characters or less, for example "Warehouse Wireless Network."
6. Set the MSTP Revision Level to an integer between zero and 65535. Most network administrators will start with one and increment it each time the MSTP configuration has to change.
7. Note the last three settings carefully. They must be identical on all switches that participate in this MSTP configuration.
8. Click on the Apply button beneath the MSTP configuration choices.

5.5.2 Set the Configuration Timing Parameters

The CIST timing parameters determine how long it will take to converge on the initial spanning tree and any similar complete reconfiguration. The parameters are:

- **Hello Time:** The interval between hello messages broadcast from one switch to the others. These messages are used to determine when a switch has gone down and a spanning tree reconfiguration is needed. Shorter intervals use up more bandwidth and allow faster response to failures. Default: 2 seconds.
- **Maximum Age:** How long forwarding information is retained in a switch before it is considered outdated and must be relearned. Shorter periods use up more bandwidth but

reduce the time that stations are unreachable when the spanning tree changes. Default: 20 seconds.

- **Forward Delay:** How long a switch must listen for BPDU messages before making a reconfiguration choice. Longer intervals make certain that the switch has heard all possible messages but lengthen the time it takes to reconfigure the spanning tree on a topology change. Default: 15 seconds.
- **Max. Hop Count:** The maximum number of hops that will be considered in finding a switch to switch path. Longer values have a better chance of finding a path to a particular destination, but take longer to converge. Default: 20 hops.

To set the configuration timing parameters:

1. Use the left menu to navigate to the CIST Configuration page (*Spanning Tree > MSTP Config. > CIST Config.*).
2. If there is a switch that is closest to the WAN and therefore should be the favored root switch, set the CIST Bridge Priority on that switch to a lower number (higher priority).
3. Set the Max Hop Count to a value appropriate for your network.
4. Set the CIST Bridge Maximum Age.
5. Set the CIST Bridge Forward Delay.
6. Set the CIST Hello Time.
7. Click on the Apply button at the bottom of the web page to record the changes.

The timing parameters have maximums and minimums that are determined, in part, by their relationship with one another in the messages sent between switches during the spanning tree algorithm.

- Maximum Age
  - minimum: twice the Forwarding Delay less two seconds; i.e. 2*(FD-1)
  - maximum: two seconds plus twice the Hello Time; 2(1+HT)
- Hello Time
  - minimum: 1 second
  - maximum: half the Maximum Age less one second; (MA/2)-1
- Forward Delay
  - minimum: half the Maximum Age plus one; (MA/2)+1
  - maximum: 30 seconds

5.5.3 Set the Port Characteristics

To speed the convergence of the spanning tree configuration or to push the spanning tree algorithm to make certain choices, the different ports characteristics can be tuned. The characteristics to be tuned are:

- **Priority:** An integer between 0 and 240. When choosing between two paths, the spanning tree algorithm will choose the path through the port with the higher priority (lower numeric value). Set the priority to a lower number to increase the likelihood that the port will be used. Defaults to 128.
- **Path Cost:** An integer between 1 and 200000000. This number represents the cost of spending a packet through this port. A higher value means that the port link is a slower speed. By default 10BaseT links have a cost of 2000000, 100BaseT links have a cost of 200000 and Gigabit links have a cost of 20000. If two port have the same priority, the spanning tree algorithm will cost the port with the lower cost.
- **STP Status:** Determines whether spanning tree protocols can work on this port. Spanning tree operations are disabled for the switch as a whole, setting this flag to Enabled will not turn on spanning tree protocols for this port along. However, setting this flag to Disabled will disable spanning tree protocols for this port, even if spanning tree protocols are enabled for the switch as a whole. Disabling a STP operations on individual ports should be done with caution, as the potential for loops and subsequent broadcast storms is significant.
- **Admin/OperEdge:** Indicates that the port connects to a device on the edge of the network, e.g., a workstation or an access port. If the port is connected to an edge unit and if this is set to True, the RSTP spanning tree algorithm will converge more quickly on a spanning tree. Defaults to False.
- **Admin/OperPtoP:** Indicates that the port connects to another switch. This variable may be set to Auto, True, or False and defaults to Auto. If it is set to Auto, the switch itself will determine a True or False value to use. If the port connects to another switch and the used value is True, then the RSTP spanning tree algorithm can more quickly reconfigure after a topology change. Unless the autodetection is failing, this is usually best left at Auto.

Priority, Path Cost, and STP Status are set using the CIST Basic Port Configuration screen (*Spanning Tree > MSTP Config. > CIST Basic Port Config*). OperEdge and OperPtoP are set using the CIST Advanced Port Configuration screen (*Spanning Tree > MSTP Config. > CIST Advanced Port Config.*).

In either case, these parameters are set using the same port configuration interface used elsewhere. That is, use the checkboxes at the top of the screen to select the ports which will be changed, select checkbox to the left of the variable that is to be modified, set the variable's value using the pull-down menus, then click on the Apply button. The port list will redisplay with the new variable values.

5.5.4 Make VLAN to MSTP Instance Assignments

MSTP spanning tree instances are identified by number, an integer between 2 and 64. Each VLAN can belong to exactly one MSTP instance. MSTP instances are created simply by assigning a VLAN to that instance number. To assign a VLAN to an MSTP instance, go to the MSTP Instance Configuration page (*Spanning Tree* > *MSTP Config.* > *MSTP Instance Config.*), enter the MSTP Instance ID number and the VLAN ID number in the top section and click on that section's Apply button. That VLAN will now be spanned in that MSTP spanning tree instance and the association between the VLAN and the MSTP instance will be displayed in the bottom half of this screen. The VLAN to MSTP Instance mappings can be deleted using the buttons in this table - Remove Instance and Remove VLAN.

5.5.5 Optional - Set Port Characteristics for MSTP Instances

The port characteristics that used by the spanning tree algorithm, Priority, Cost, and STP Status, and which were discussed in *Set the Port Characteristics on page 5-8*, can also be set on a per-MSTP-instance basis.

To set these for a particular MSTP instance, go to the MSTP Instance Configuration page (*Spanning Tree* > *MSTP Config.* > *MSTP Instance Config.*), and enter the MSTP instance number below the heading "MST Instance Port Config" and click on the Apply button to the right. A new screen will display titled *MST Instance Port Configuration* which will allow configuration of these parameters in exactly the same was as they were configured in *Set the Port Characteristics on page 5-8*.

The switch's priority as used for selection of the root switch within a spanning tree may also be set for any particular MSTP spanning tree instance. Go to the MSTP Instance Configuration page (*Spanning Tree* > *MSTP Config.* > *MSTP Instance Config.*), and enter the MSTP instance number below the heading "MST Instance Port Config" and click on the Apply button to the right. A new screen will display titled *MST Instance Configuration.* Use the drop down menu to set the MSTI Bridge Priority. It will default to 8000. A lower numeric value will increase the likelihood that this switch is selected as the root switch for this MSTP spanning tree instance.

5.6 Displaying MST Spanning Tree Instance Status

The roles of each port in a MSTP spanning tree instance can be displayed. Go to the MSTP Instance Configuration page (*Spanning Tree* > *MSTP Config.* > *MSTP Instance Config.*), and enter the MSTP instance number below the heading "MST Instance Topology Info" and click on the Apply button to the right. A new screen will display with the heading *MST Instance Topology Information.* Each of the ports will be listed as well as the roles it plays in the specified MSTP instance.

5.7 Static Forwarding Database

For each VLAN, the ES3000 listens to the packets received at each port and maintains a list of MAC addresses from which packets have been received. This list of VLANs, ports, and MAC addresses is the forwarding database (FDB).

When a packet is received on a VLAN, if there is an entry in the forwarding database for that VLAN and that destination MAC address, the packet is forwarded to that port. If a packet is received on a VLAN for a MAC address which is not listed in the forwarding database for that VLAN, the packet is forwarded to all ports on the VLAN.

Because equipment moves, entries in the FDB cannot be permanent. Entries normally time-out after 300 seconds. Permanent entries may be made by the network administrator. To make a permanent entry:

1. Select, in the lefthand menu, select *Spanning Tree* > *Forwarding DB* > *Add Static FDB Entries*.
2. Enter the port, VLAN ID number, and MAC address for the static FDB entry.
3. Press the Apply button.
4. Save the configuration. *System Admin.* > *Tools* > *Save Config.*

6

VLANs

6.1 VLAN Overview

6.1.1 Physical Local Area Networks

A physical local area network (LAN) is also a broadcast domain, a section of a network in which broadcast packets are delivered to all end-stations. In a physical LAN, the cabling and the router define the range of the broadcast domain. All end-stations must be physically connected to the router. For an end-station to be on several physical LANs, it must have multiple network interface cards.

This physical connection limits the usefulness of LANs. If a physical LAN gets too large, the broadcast packets and the responses to them consume a large part of the network bandwidth, clogging the network. If the LAN is used as a security device, all users of a particular type must be close together or multiple wiring systems must be maintained.

6.1.2 Virtual LANs

Virtual LANs (VLANs) are broadcast domains which are defined by the configuration of network equipment rather than cabling. The network administrator determines which end-stations are on which VLANs by software changes rather than cabling decisions. On the ES3000 switch, there are two kinds of VLANs: manual VLANs and dynamic VLANs.

A manual VLAN is a group of ports that are defined by the network administrator as being on the same VLAN. Broadcast packets are repeated to all of the ports on the same VLAN. The packets pass back and forth on this VLAN are usually regular Ethernet packets, with no additional tags on the packet. These VLANs are compatible with all network equipment, but a port may belong to no more than one VLAN of this type because, without a tag of some kind, there is no way of distinguishing which VLAN a packet is travelling on when it enters the switch.

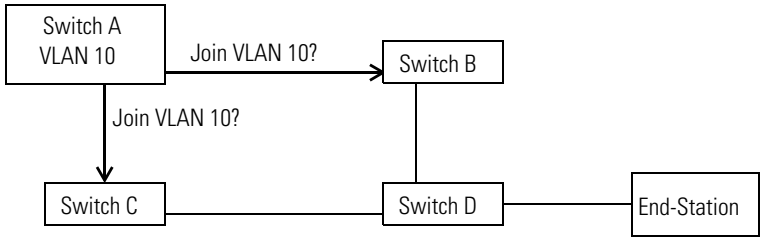
However, if the packets are tagged with the identity of the VLAN, significant advantages derive from the tagging. First, a port may belong to more than one VLAN. Second, VLANs can span switches. Third, VLANs can be created on demand. Finally, end-stations can be moved, at will, within a group of switches, and automatically remain on their home VLAN.

The VLAN tagging standard is 802.1Q. Packets are marked with a number between 2 and 4094, with 0, 1, and 4095 being reserved. Unfortunately, the tag increases the maximum packet size by four bytes. Network equipment manufactured before 1998 may see these packets as malformed and may drop them. For this reason, ports on most 802.1Q compatible equipment can be configured to strip the tagging when sending a packet and to add a tag when a packet is received on that port. Such ports must have a default VLAN specified. A tag for this VLAN will be added to the incoming untagged packets before sending them out on the VLAN.

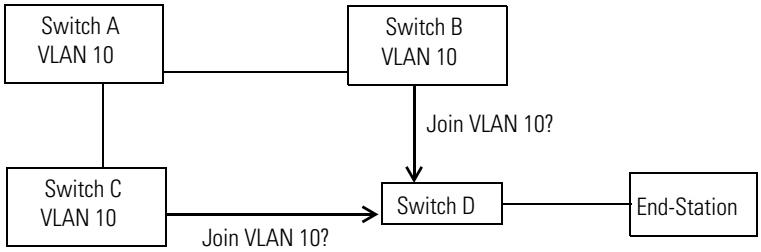
6.1.2.1 Dynamic VLANs (GVRP)

Other than allowing a port to be part of more than one VLAN, most of the advantages of tagged VLANs come from allowing the network equipment to configure the VLANs automatically. The VLANs configure themselves by exchanging GARP[1] VLAN registration protocol (GVRP) messages. All GVRP-configured VLANs must be use tagged packets.

When a GVRP-capable switch is started, it sends GVRP packets out all ports which are enabled for dynamic VLANs. These packets identify, by VLAN number, all the VLANs on that switch.

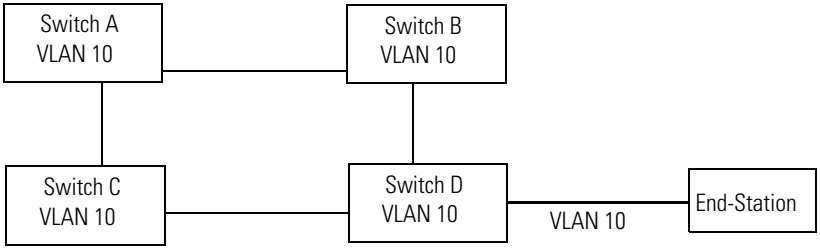


When the next layer of switches get this packet, they join the VLAN on the first eligible port to receive the GVRP packet. Those switches then send GVRP packets out all ports other than the ports that have already joined the VLAN.

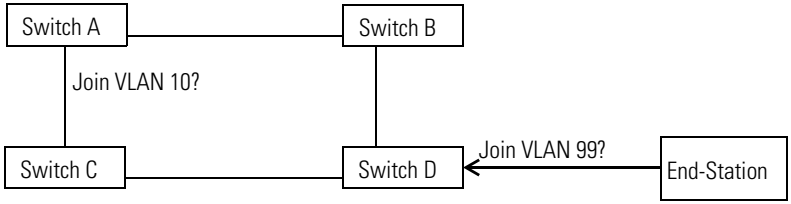


Those switches then send out GVRP messages on all of their eligible ports as well. When the message reaches an end-station with a 802.1Q-enabled network interface that has been configured to be part of that VLAN, or if the message reaches a switch that has been manually configured for a port to an end-station to be part of that VLAN, then that port will also join the VLAN.

1. GARP: General Attribute Registration Protocol. GVRP is a use of the more general GARP.



A GVRP message can also start from an end-station with an 802.1Q-enabled network interface and will propagate in the same way as it would if the message had started with a switch instead of an end-station.



If all of the network equipment between two end-stations is configured to allow it, two end-stations on the same VLAN can be attached to the network at any location and the GVRP messages will enable them find each other and be on the same VLAN.

6.2 Creating and Configuring a VLAN

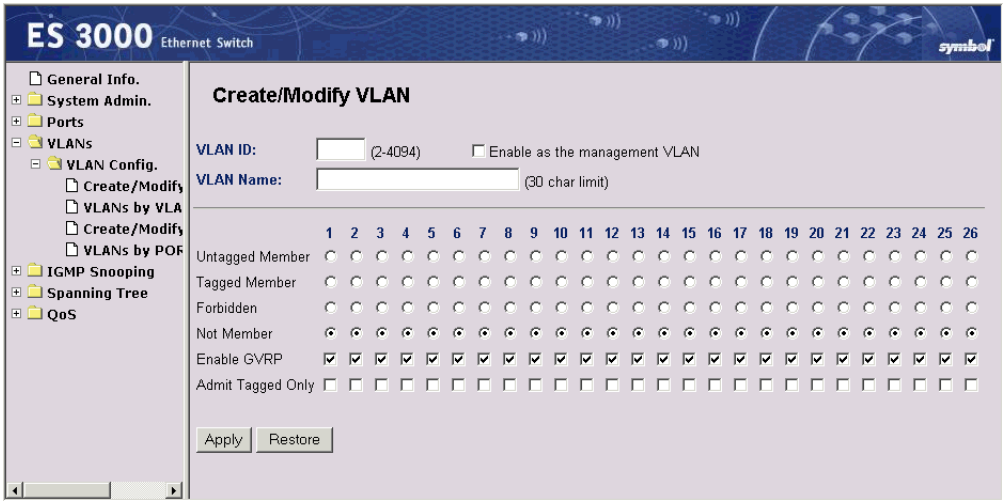
6.2.1 Create/Modify VLAN Page

VLANs are created on the Create/Modify VLAN page (*VLANs > VLAN Config. > Create/Modify VLAN*) in either the web or menu interface.

A VLAN is created by specifying the following parameters:

- **VLAN ID:** An integer between 2 and 4094. This number will be used to identify the VLAN in GVRP packets and will be the same on all switches and devices where the VLAN is active.
- **VLAN Name:** A string up to 30 characters in length. This string has no function other than to make it easier to identify VLANs on the switch. The string is not passed between network devices and can be different on different switches.

- **Tagged Members:** Ports on the switch which must be part of the VLAN and which will receive tagged packets from the switch.
- **Untagged Members:** Ports on the switch which must be part of the VLAN and which will receive untagged packets from the switch. This option is usually used to connect to an end-station which does not understand 802.1Q tagging. A port may only be an untagged member of one VLAN.
- **Forbidden Ports:** Ports on the switch which may not be part of the VLAN.
- **Not Members:** Ports on the switch which are not now part of the VLAN but which may be added to the VLAN if GVRP packets are received which request that the port join.
- **Enable GVRP:** If Enabled, GVRP packets will be sent out this port to invite other switches to join this VLAN.
- **Admit Tagged Only:** If enabled, the port will ignore untagged packets entering the port.



A port can only be an untagged member of one VLAN at a time. If a port is added as a untagged member of a second VLAN, it will be removed from membership in the previous VLAN in which it was an untagged member.

If a port is an untagged member of a VLAN and also a tagged member of one or more VLANs and if an untagged packet is received on that port, then packet is assumed to be from the VLAN which does not require tags. Before that packet is passed to any port that requires tagging, the packet will be tagged with the VLAN ID of the VLAN in which the port is an untagged member.

One and only one VLAN can also be marked as the Management VLAN. The default is VLAN 1, the VLAN which contains all ports. This default allows management access to the switch from all ports. If the Management VLAN is set to another VLAN, management of the switch will be restricted to ports on this VLAN.

Changing the Management VLAN to a VLAN which does not include the port from which the change was made will result in the switch becoming unavailable on that port. If this happens, further management contact with the switch will have to be made through a port on the new Management VLAN.

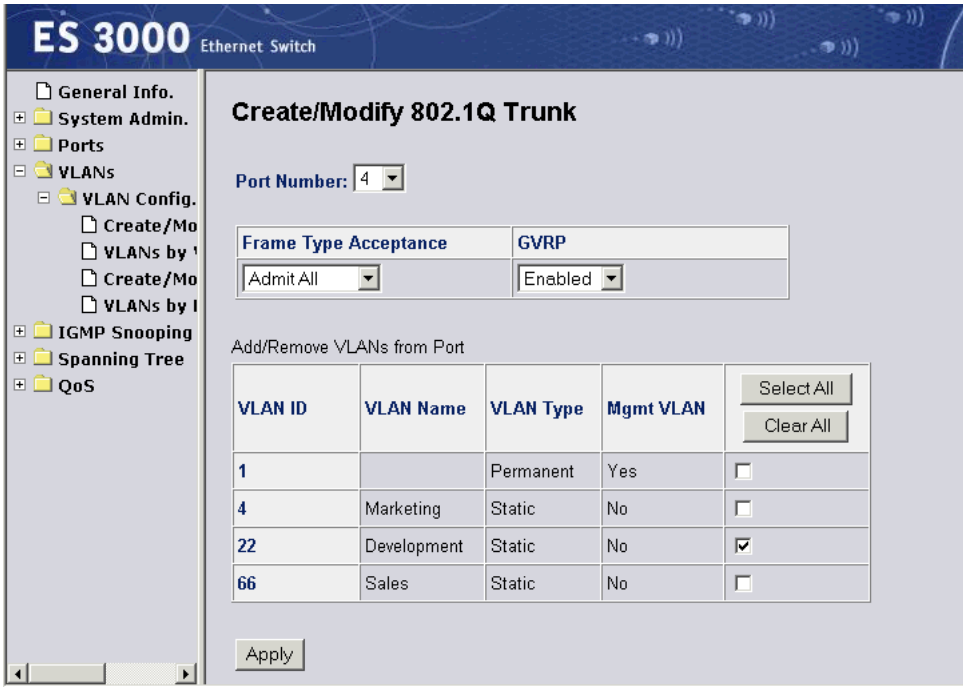
After the VLAN components have been specified, use Apply to create the VLAN. After the VLAN has been created, the individual characteristics of the ports can be specified on the VLAN Configuration Page.

6.3 Displaying and Modifying VLAN Information

VLAN information may be displayed by port number (*VLANs > VLAN Config. > VLANs by Port*) or by VLAN ID number (*VLANs > VLAN Config. > VLANs by VLAN-ID*). In the web interface's VLAN ID display, each VLAN is shown with a Modify link. The Modify link leads to the Create/Modify VLAN page with the VLAN set. This page allows ports to be moved from Member Ports to Forbidden Ports to Not Members. See *Create/Modify VLAN Page on page 6-4*, above.

6.4 Create/Modify 802.1Q Trunk

IEEE 802.1Q is the standard for encapsulating packets and marking them with VLAN information before sending them across a link between two switches. This screen allows modification of the encapsulation behavior on a port-by-port basis rather than on a VLAN-by-VLAN basis. It can also be used to control VLAN membership on a port-by-port basis.



When a port number is selected, the information for that port is displayed.

- Frame Type Acceptance: Admit All or Tagged Only.
  If Tagged Only, incoming packets which are not tagged with 802.1Q VLAN information will be dropped. If Admit All, then all packets will be admitted.
- GVRP: Enabled or Disabled.
  If Enabled, the switch will allow and respond to dynamic VLAN invitations which it receives over this port in GVRP format. If Disabled, these packets will be dropped.

All current VLANs on the switch are displayed in table format. The check boxes to the right indicate whether or not this port is currently a member of that VLAN.

To modify the VLAN characteristics of the port, change the display and then click the Apply button.

7

Link Aggregation

7.1 Link Aggregation Overview

Link aggregation allows the ES3000 switch to bundle individual physical links into a single logical link, called a *link aggregation group*, or group. Link aggregation provides increased bandwidth and creates redundant links between linked devices (partners). It also provides load balancing, where processing and communication are distributed across links within a group so that no single link is overwhelmed.

Link aggregation on the ES3000 switch can create logical links either between switches or between switches and servers or routers that are also configured for link aggregation.

The standard for link aggregation is IEEE 802.3ad. This standard also provides for a dynamic signalling protocol, the Link Aggregation Control Protocol (LACP). LACP allows linked devices to dynamically configure and maintain link aggregation groups. The ES3000 switch uses LACP to establish 802.3ad compliant link aggregation groups.

7.2 Implementing Aggregate Links

The ES3000 switch allows the administrator to create link aggregation groups that include up to eight physical ports in a single logical link. The administrator can define a maximum of six link aggregation groups. Each port can participate only in one link aggregation group.

The ports within a link aggregation group must of the same type, either 100BaseT or gigabit. The switch prevents groups that include both 100BaseT and gigabit ports. When the administrator creates a link aggregation group, the switch forces all ports within a group to full duplex mode at the highest speed allowed for the port.

All ports in a group must belong to the same set of VLANs. For example, if port 4 belongs to VLANs 1, 3, and 14, and port 5 belongs to VLANs 1 and 14, the switch does not allow the creation of a link aggregate group including both ports 4 and 5.

To avoid broadcast storms or loops in the network when configuring a link aggregation group, disable or disconnect the ports before adding or removing them from a group. The ports can be re-enabled or connected after the group is defined.

For spanning tree protocol (STP), link aggregation groups function as a single virtual port. Any changes to one port in a group are applied to all ports in the group.

7.2.1 Link Aggregation Mode

The LACP provides dynamic and static modes of link aggregation.

The dynamic mode allows the switch to negotiate with partner interfaces to determine whether they can form a mutual link. In dynamic mode a link aggregation group can be either active and passive. A group in the active mode initiates the negotiation, while one in the passive mode waits for negotiation from the partner side. A successful negotiation requires at least one end of the aggregation link to be in active mode. If both ends are in passive mode, negotiation never begins.

In the static (or manual) mode, the LACP forces all ports to join the link aggregation group without LACP negotiation.

7.2.2 Defining a Link Aggregation Group

Use the Add Group page (*Ports > Link Aggregation > Add Group*) to add new link aggregation groups, and modify or delete existing groups.

7.2.2.1 Adding a Link Aggregation Group

To set up a new link aggregation group, supply the following information on the Add Group page:

- **Group Admin Key:** A unique key that identifies the link aggregation group. The Spanning Tree and Port Configuration pages use this key to display the group a port belongs to. The value is an integer in the range 0-65535.
- **Group Mode:** The LACP aggregation mode. The administrator can select LACP Active, LACP Passive, or Manual. See “Link Aggregation Mode” on page 3. The default is Manual.
- **Group Member:** The ports to select for group membership. Click Apply to create the group. If the selected ports do not form a valid group, the web interface generates an error message and denies the creation of the group. See “Implementing Aggregate Links” on page 2 for a description of the prerequisites for creating a valid group.

Once the administrator has created groups, they appear on the display at the bottom of the Add Group page, where the administrator can view the key, mode, and port list for the group. If the mode is LACP Active or LACP Passive, click the LACP Status button for a group to view detailed status information.

7.2.2.2 Modifying a Link Aggregation Group

On the Add Group page, the administrator can modify a link aggregation group in one of two ways:

- By clicking the Modify button next to the group. When the Link Aggregation Modify page appears, the administrator can change the group mode and then either add or remove ports for the group. Click Apply to modify the group. If selected ports do not form a valid group, the web interface generates an error message and refuses to make the change.
- By entering an existing Group Key in the Group Key box. The administrator can select a new mode, and add ports to the group directly on the Add Group page. Click Apply to make the changes. Take care to set the mode appropriately or the mode returns to the default of Manual.

7.2.2.3 Deleting a Link Aggregation Group

To delete a group using the Add Group page click the group's Modify button. When the Link Aggregation Modify page appears, de-select all group members, and click Apply. The web interface returns to the Add Group page, which no longer displays the group.

7.2.3 Setting Priorities

The LACP uses priorities to determine which links of a group take precedence for LACP transmission. It also uses priorities to determine which port to use if one of the links fails. The combination of system and port priority determines which ports take precedence when a link fails.

7.2.3.1 Setting System Priority

In LACP negotiation, the partner with the highest system priority determines which links are active and which are in standby for each link aggregation group.

Using the System Priority page (*Ports > Link Aggregation > System Priority*) the administrator can set the global system priority value for LACP. Valid priorities range from 0 to 65535, where the lower value has the higher priority. The default system priority is 1.

7.2.3.2 Setting Port Priority

Using the Port Priority page (*Ports > Link Aggregation > PortPriority*) the administrator can set the priority value for individual ports. The lower the value, the higher the port priority. When two ports have equal priority, the lower port number has the higher priority. The default priority for all ports is 1.

The value can range from 0 to 255. Enter port and priority values and click Apply. The port priorities are displayed over successive pages. Click the Next button to see additional ports.

8

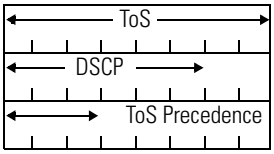
QOS Management

8.1 QoS Overview

The ES3000 implements IEEE 802.1p Quality of Service (QoS) processing. QoS policies examine packets and classify them. The classification is used to drop packets or to remark packets. The possible markers are Class of Service (CoS) Priority, Type of Service (ToS) Precedence, and Differentiated Services Code Points (DSCP). For each port, the outgoing packets are then placed in four output queues based on CoS priority. The queues are serviced using a strict queueing algorithm. See *Configuring QoS Queues on page 8-11* for details on the algorithm.

8.1.1 QoS Markers

Two of the settable markers, ToS Prececedence, and DSCP, are not independent. The DSCP are encoded in the top six bits of the ToS. The ToS Precedence is encoded in the top three bits of the ToS, as shown below:



The COS priority is encoded in a different location, in first three bits of the Tag Control Infomation (TCI) field of the 802.1p tag in the Ethernet frame.

8.2 Creating a QoS Policy

A QoS policy consists of a classifier, one or more actions, a port list and a sequence number. The classifier determines which packets are affected by the policy. The action determines what is done with the policy. The policy applies only to the traffic coming over the ports in its port list. Policies are applied in sequence order.

There are three types of actions: in-profile actions, out-profile actions, and no-match actions.

- In-profile actions effect packets that are in-bound to the switch, ingress packets. In-profile actions can either drop a packet or mark it with a DSCP value, CoS priority, or a ToS precedence.
- Out-profile actions effect packets that match the characteristics specified by the classifier and which exceed bandwidth or burst size limits specified in the out-profile. The actions can be either to drop the packet or to change its DSCP value, usually to drop the DSCP value.

- No-match actions act on packets that are in-bound to the switch and which *do not match* the characteristics specified by the classifier.

Each of the components of a policy—classifier, action, port list—is identified by an index when it is created. After all of the components have been created, the policy itself is created by specifying a sequence number and the index numbers of each of its components. A written list of the classifier, action, and port list indices is helpful during this step.

Up to sixteen policies can be operative for each port, but four of these policies are reserved for system use. No more than twelve uder-defined policies can apply to a particular port.

After creation, policies are applied in sequence order. When a packet is matched with a policy which specifies an in-profile action or an out-profile action, then that action is taken and no more policies are considered for that packet.

8.2.1 Creating a QoS Classifier

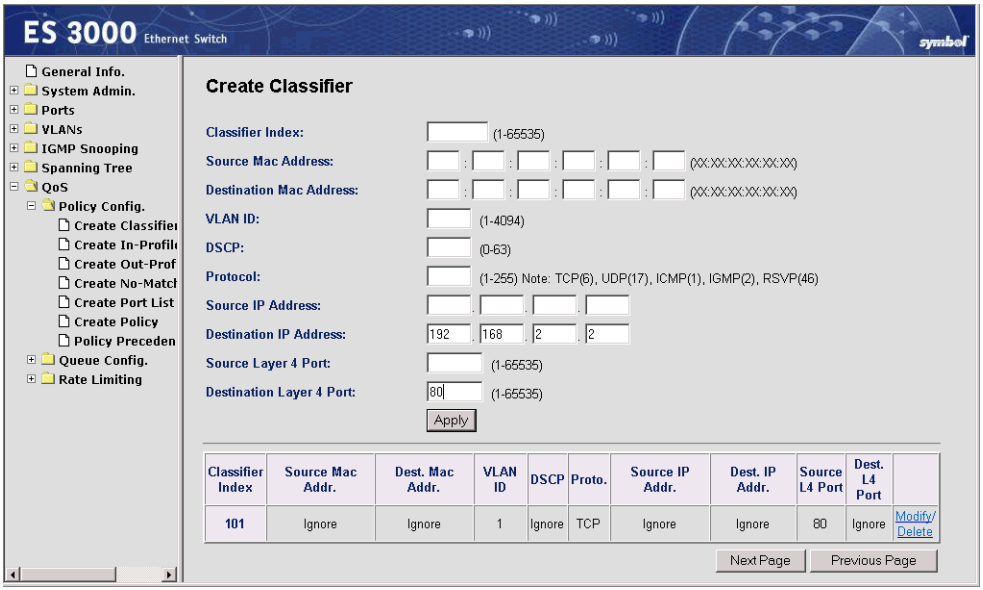
Classifiers determine which packets are effected by a QoS policy. To create a classifier, go to the Create Classifier page in the web interface (*QoS > Policy Config. > Create Classifier*) or the menu interface. Classifiers can also be created using the `diffserv classifier` command in the CLI.

The following parameters can be specified in a classifier:

- Source MAC address
- Destination MAC address
- VLAN ID number
- DSCP value: The existing Differentiated Services Code Point in the packet
- Protocol number: The Internet Protocol version 4 protocol number. See *Port Numbers and Protocol Numbers on page 8-13*.
- Source IP address
- Destination IP address
- Source port: The source Ethernet Layer 4 port number. See *Port Numbers and Protocol Numbers on page 8-13*.
- Destination port: The destination Ethernet Layer 4 port number.

If more than one parameter is specified in a classifier, both must match for the classifier to apply. Any parameter which is not specified is ignored for purposes of matching the classifier to the traffic. For example, a classifier which specified destination IP address as 192.168.2.2 and specified no other parameters, would apply to all traffic with that destination IP address. A classifier which specified

the destination IP address as 192.168.2.2 and the destination layer 4 port as 80, would apply only to port 80 traffic bound for that IP address.



The format for the CLI command is

```
diffserv classifier <id> [src-mac <MAC>][dst-mac <MAC>]
[vlan-id <vid>]  [dscp <value>][protocol <pro-num>]
[src-ip <ip>][dst-ip <ip>] [src-port <port>][dst-port <port>[
```

8.2.2 Creating a QOS In-Profile Action

If a QoS policy has an in-bound profile action, that action will apply to any in-bound traffic that matches the classifier set for that QoS policy. The in-profile action can be any one of the following:

- Drop the packet.
- Set the packet's DSCP bits to a number between 0 and 63.
- Set the packet's ToS precedence to a number between 0 and 7.
- Set the packet's CoS priority to a number between 0 and 7.

The upper three bits of the DSCP are used to encode the ToS precedence, so that the following equivalences hold:

A DSCP Value of	Implies ToS Precedence of
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

The CoS priority determines the output queue for the packet and therefore may also effect the speed with which the packet is sent from the switch.

The ToS Precedence and the lower three bits of the DSCP have no direct effect on the processing of the packet within the ES3000. They may be used by other QoS aware devices that transmit the packet.

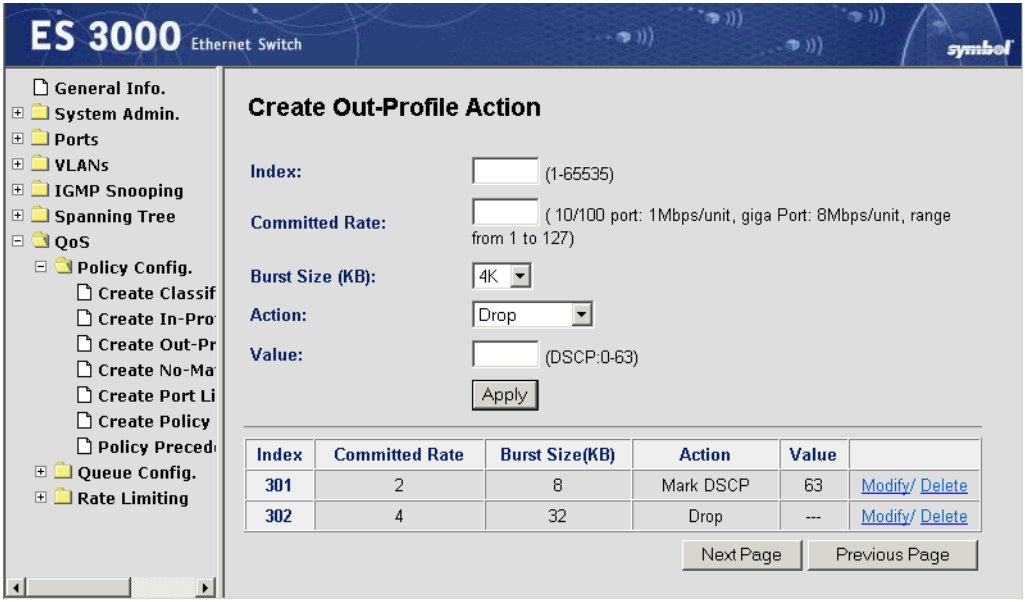
In-profile actions can be created through the web interface (*QoS > Policy Config. > Create In-Profile Action*), the menu interface, or the `diffserv inprofile` command in the CLI. The format for the CLI command is:

```
diffserv inprofile <id> {drop | dscp <value> | precedence <value>|
cos <value>}
```

8.2.3 Creating a QOS Out-Profile Action

An out-profile action specifies what is to be done with a class of traffic if it exceeds a specified level of traffic. The traffic level is specified by both traffic in bits per second and in the burst size in kilobytes. Exceeding either of these parameters causes the traffic to be considered out of profile.

The combination of a classifier with an in-profile action with one DSCP value and an out-profile action with a higher DSCP value (lower priority) has the effect of giving that class of traffic faster processing as long as the volume of the traffic stays under the traffic limits specified in the out-profile.



Out-profile actions can be created through the web interface (*QoS > Policy Config. > Create Out-Profile Action*), through the menu interface, or by using the `diffserv outprofile` command in the CLI. The format for the CLI command is:

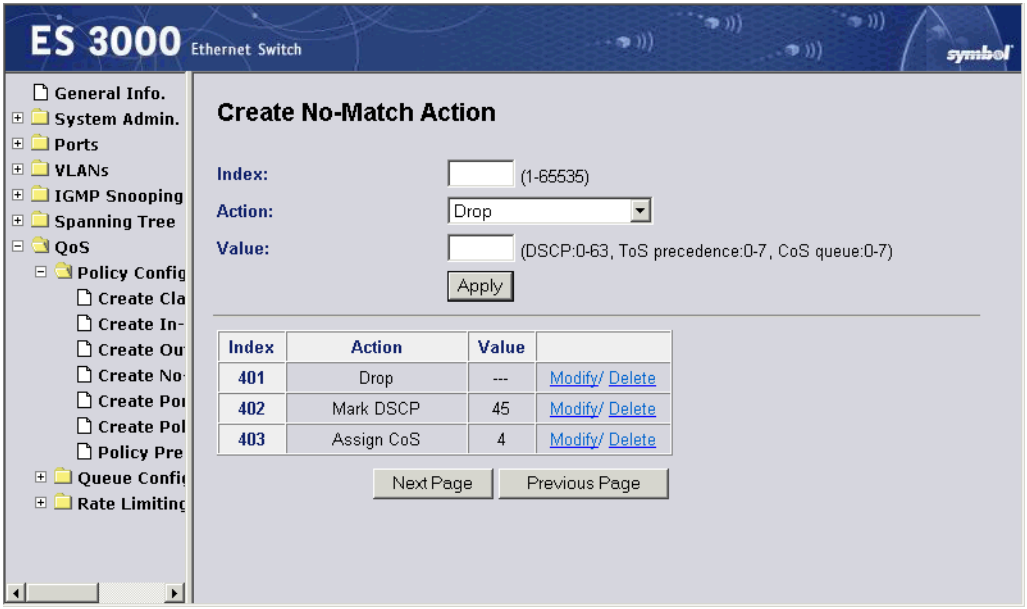
```
diffserv inprofile <id> {drop | dscp <value> | precedence <value>
| cos <value>}
```

The committed rate is specified in megabits per second for the 10/100BaseT ports and in 8 megabit per second units for the Gigabit ports. A committed rate value of four has the meaning of 4 megabits per second when applied to a 100baseT port and it has the meaning of 32 megabits per second when applied to a Gigabit port.

8.2.4 Creating a QOS No-Match Action

If a QoS policy has a no-match profile action, that action will apply to any in-bound traffic that does not match the classifier set for that QoS policy. The no-match actions are exactly the same as the in-profile actions, that is, any one of the following:

- Drop the packet.
- Set the packet's DSCP bits to a number between 0 and 63.
- Set the packet's ToS precedence to a number between 0 and 7.
- Set the packet's CoS priority to a number between 0 and 7.



No-match actions can be specified through the web interface (*QoS > Policy Config. > Create No-Match Action)* the menu interface, or the `diffserv nomatch` command in the CLI. The CLI command take the form:

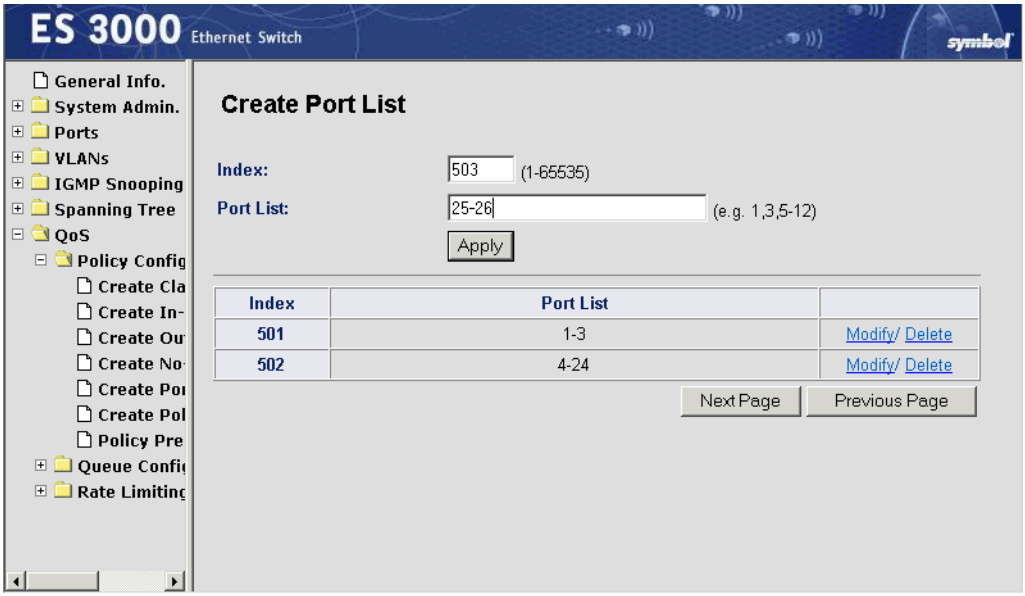
```
diffserv nomatch <id> {drop | dscp <value> | precedence <value> |
cos <value>}
```

8.2.5 Creating a QOS Port List

QoS policies apply to a specified list of ports. The port list may be specified through the web interface (*QoS > Policy Config. > Create Port List*), menu interface, or the `diffserv portlist` command. The format of the CLI command is:

```
diffserv portlist <datapath-id> <portlist>
```

where `datapath-id` is an index and `portlist` is a list of port numbers or port number ranges, separated by commas.



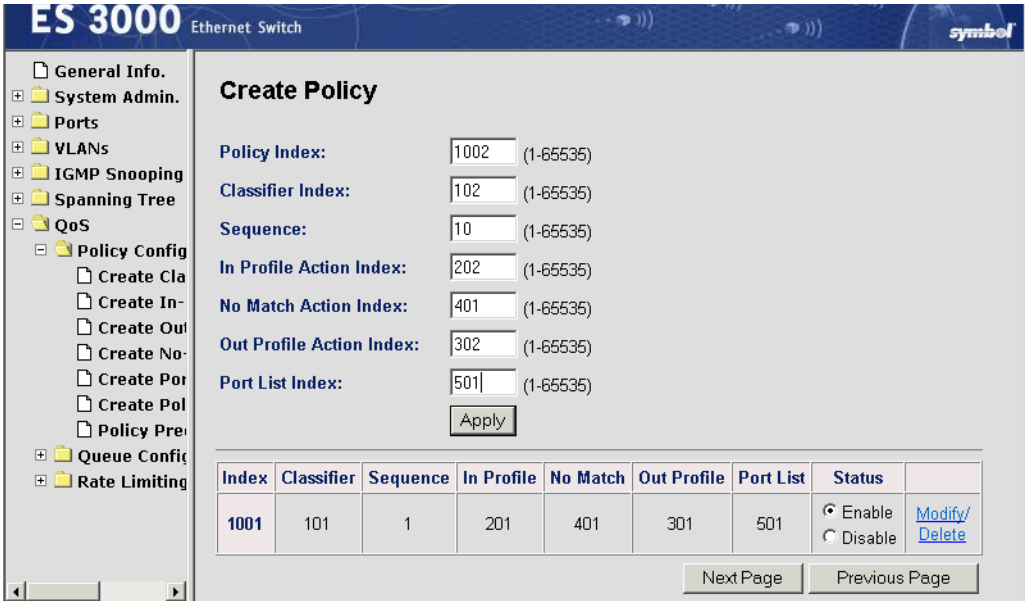
8.2.6 Creating a Qos Policy

After all of the required classifiers and policies have been specified, a QoS policy can be created. The policy consists of a classifier, a sequence number, a port list, and one or more actions. The sequence number determines the order in which the policies are applied. All rules apply, in order, that can apply. If more than one QoS rule applies to a packet and if the QoS rules conflict in the actions to be taken, then action take will be that of the last rule to be applied.

The policies are specified in the web interface, the menu interface (*QoS > Policy Config. > Create Policy*), or using the `diffserv policy` command in the CLI. The format of the CLI command is:

```
diffserv policy <index> portlist <index> classifier <index>
policy-precedence <value> [inprofile <index>] [nomatch <index>]
[outprofile <index> ]
```

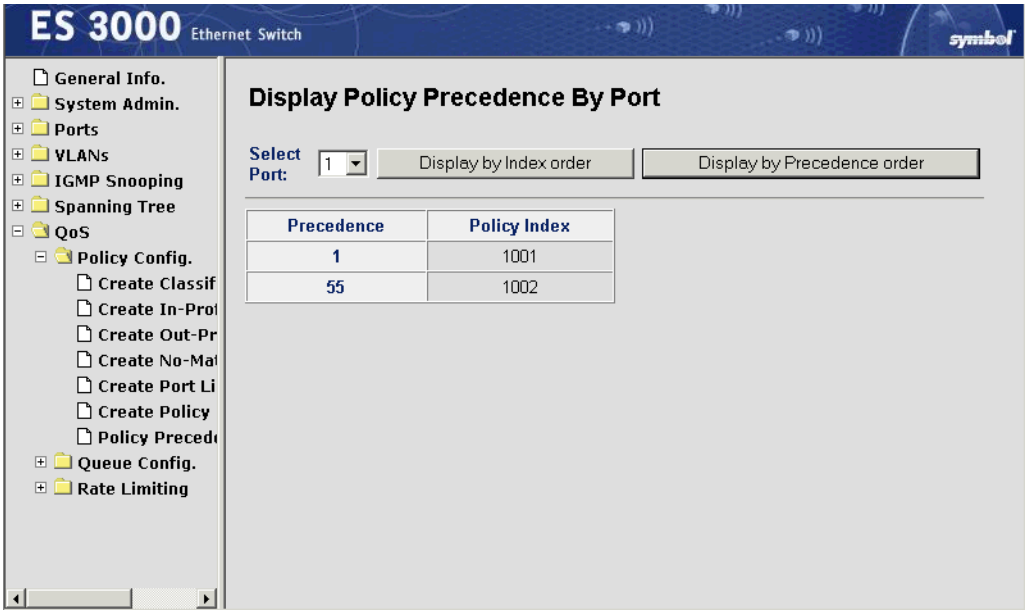
No more than twelve QoS policies may apply to a single port number.



8.3 Displaying QoS Policies

After the QoS policies have been set, the policies which apply to a particular port can be displayed using the Policy Precedence display in the web interface (*QoS > Policy Config. > Policy Precedence*), menu interface, or the CLI command:

```
show diffserv policy-precedence port <port num> sort {policy-index | precedence}
```



8.4 Configuring QoS Queues

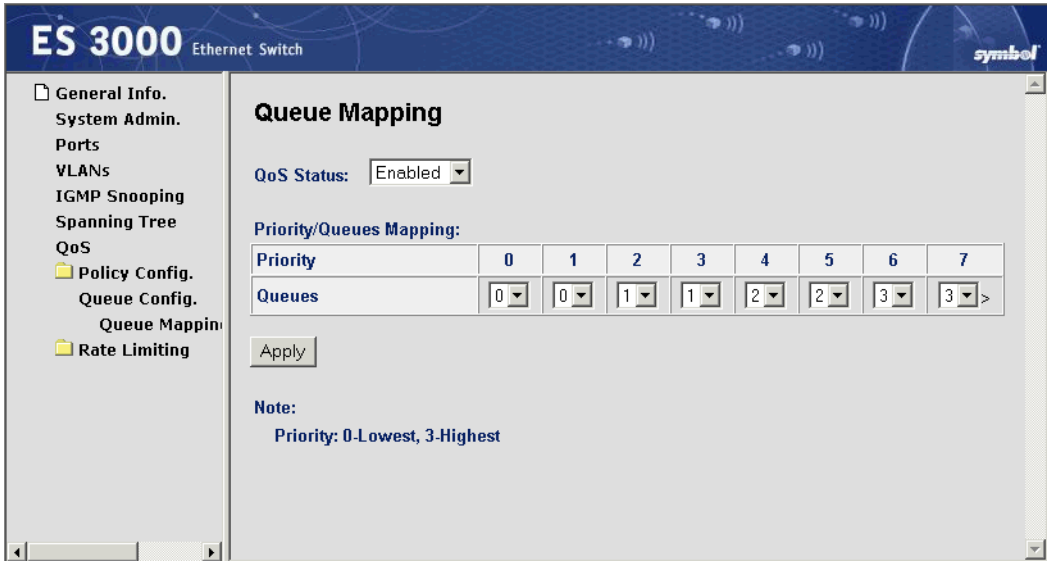
Each port has four output queues. The packets are sorted into the output queues depending on their CoS priority values. See *Creating a QOS In-Profile Action on page 8-4* a discussion of CoS priority.

The queues are serviced using a strict queuing algorithm. Packets in the highest-priority queues, starting with queue #3 are serviced before any packets from a lower-priority queue.

The queues are initially configured as follows:

Queue	CoS values
3	6,7
2	4,5
1	2,3
0	0,1

CoS priority values of 6 and 7 are usually reserved for control communication between network equipment.



The mapping of CoS priority values to output queues can be changed using the Queue Mapping display (*QoS > Queue Config. > Queue Mapping*) or the `priority-queue` command. The format of the CLI command is

```
priority-queue cos-map <traffic class> <priority>
```

8.5 QoS Configuration Example

Assume a network administrator is trying to improve service for VoIP packets using application port 1071. The following steps would create a QoS rule which:

- Applies only to switch ports 4 to 24
- Assigns all traffic with port number 1017 to CoS priority level 5, up to a limit of 4 megabits per second
- Assigns the traffic on port number 1017, but above that traffic limit, to CoS priority 3
- Assigns all other traffic to CoS priority level 1

The steps are given in CLI command:

1. Set up a classifier for a Ethernet Layer 4 destination port of 1071:

   ```
   diffserv classifier 101 dst-port 1071
   ```

2. Create an in-profile action which assigns a CoS priority level of 5:

   ```
   diffserv inprofile 201 cos 5
   ```

3. Create an out-profile action which assigns a DSCP value of 31. This is the equivalent of a CoS value of 3.

   ```
   diffserv outprofile 301 committed-rate 4 burst-size 16 policed-dcsp
   31
   ```

4. Create a no-match which assigns a CoS priority level of 1:

   ```
   diffserv nomatch 401 cos 1
   ```

5. Create a port list for ports 4 to 24:

   ```
   diffserv portlist 501 4-24
   ```

6. Create a policy using the various parts just created:

   ```
   diffserv policy 1001 portlist 501 classifier 101 policy-precedence
   10 inprofile 201 nomatch 401 outprofile 301
   ```

The policy was created with a policy precedence number of 10 so that later policies could override the no-match policy and assign higher priorities to control communications between switches and routers.

8.6 Port Numbers and Protocol Numbers

Both port numbers and protocol numbers are maintained by the Internet Assigned Numbers Authority (IANA). For your convenience some of the most often used protocol and port numbers are listed below.

In the IP header, there is a field, called Protocol, to identify the next level protocol. This is an 8 bit field.The most often used protocol numbers are:

Protocol Number	IP Protocol
1	ICMP: Internet Control Message Protocol. Used for *ping*.

Protocol Number	IP Protocol
2	IGMP: Internet Group Management Protocol
6	TCP: Transmission Control Protocol
17	UDP: User Datagram Protocol
41	IPv6: Internet Protocol, version 6
46	RSVP: Reservation Protocol
80	ISO-IP: ISO Internet Protocol

A complete list of protocol numbers is available at http://www.iana.org/assignments/protocol-numbers.

Ports are used in TCP and UDP to name the ends of logical connections which carry long term conversations. The IANA manages only the first 1024 port numbers. Port numbers above 1024 are available for ad hoc use by users. The first 1024 ports are called the Well Known Ports. Some of the Well Known Ports are:

Port Number	Application
20,21	FTP: File Transfer Protocol
23	Telnet
25	SMTP Simple Mail Transfer Protocol
53	DNS: Domain Name Service
69	TFTP: Trivial File Transport Protocol
80	HTTP: Hypertext Transport Protocol
109, 110	POP: Post Office Protocol
161,162	SNMP: Simple Network Management Protocol
280	HTTP management
443	HTTPS: HTTP over TLS/SSL

A complete set of assigned port numbers is available at http://www.iana.org/assignments/port-numbers.

9

Port Security

9.1 Understanding 802.1x Port-Based Security

The ES3000 switch provides port-based security to prevent unauthorized clients from accessing a network. This security feature implements the IEEE 802.1x port-level authentication standard.

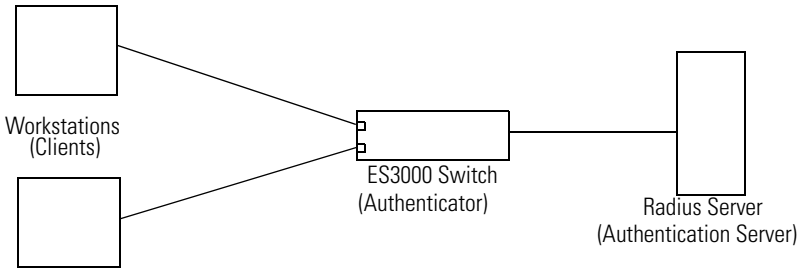


Figure 9.1 802.1x Device Roles

In 802.1x port-based authentication, the network devices have specific roles, as shown in *Figure 9.1*:

- **Client/Supplicant:** The device that requests access to the network. The client uses the Extensible Authentication Protocol (EAP) to communicate with the authenticator. In the IEEE 802.1x specification, the terminology used for *client* is *supplicant*.
- **Authenticator:** The device that controls access to the network using 802.1x authorization. The authenticator receives a username and password from the client, then passes a request for authorization to the authentication server. Based on the results from the authentication server, the authenticator allows or prohibits network access. In this scenario, the ES3000 switch can function as an authenticator.
- **Authentication Server:** The authentication server validates the username and password, and notifies the authenticator whether access is granted or denied. The Authenticator can also provide access privileges, which grant specific network privileges to the client, such as VLAN access.

The switch's 802.1x implementation currently supports standard RADIUS (Remote Access Dial-In Service) authentication servers. The EAP types supported include MD5, EAP-TLS, and PEAP.

To configure 802.1x port-based security on the ES3000 switch, configure the RADIUS server parameters to define switch-to-server communication and the 802.1x authentication parameters for each port.

9.2 Configuring Switch-to-RADIUS-Server Communication

Use the Radius Configuration page (*Ports > Port Security > Radius*) to configure RADIUS server parameters on the switch. This page includes the following parameters:

- **Server IP address:** The IP address of the remote RADIUS server.
- **Shared Secret:** The authentication and encryption key used between the switch and the RADIUS server. This key is a text string that must match the encryption key used on the RADIUS server.
- **Response Time:** The number of seconds that the switch waits for a response from the RADIUS server before attempting a retransmission. The range is 1 through 120. The default is 10 seconds.
- **Maximum Retransmission:** The number of times the switch sends a request before giving up. The range is 1 to 254. The default is 3.

9.3 Configuring 802.1x Port-Based Authentication

Use the 802.1x Configuration page (*Ports > Port Security > 802.1x*) to configure 802.1x parameters for individual ports on the switch, which specify how authentication is handled for each port. This page includes the following parameters:

- **NAS ID:** The Network Access Server (NAS) identifier. Identifies the switch as an 802.1x authenticator to the server.
- **Initialize:** Initializes 802.1x on the port specified in the Port parameter.
- **Re-auth Initialize:** Requests a manual re-authentication of the port specified in the Port parameter.
- **Port:** The port number to which the other parameters on this page apply. Select the port number (1-26). The default is port 1.
- **Port Status:** The 802.1x authorization status of the port. Specifies whether transmission is Authorized or Unauthorized. The value reflects Port Control authorization and the outcome of the authorization process. This parameter cannot be changed.
- **Port Control:** The port control state, which indicates whether authorization is allowed. Set this parameter to one of three possible values:
  - Force Authorized: Disables the 802.1x authentication. Port Status transitions to Authorized, and allows normal traffic through the port. This is the default for all ports.
  - Force Unauthorized: Forces the port into an unauthorized state. Port Status transitions to

Unauthorized. The switch ignores all attempts by the client to authorize.

- Auto: Enables 802.1x authentication, which causes the port to begin in the unauthorized state. In the unauthorized state, only EAP over LAN (EAPOL) frames are sent through the port until the RADIUS server authorizes the connection. When the connection is authorized, the switch transitions Port Status to Authorized, and permits normal traffic through the port. If authentication fails, the Port Status remains in the Unauthorized state, but the client can attempt additional authentication requests. When a client logs off the network with an EAPOL-logoff request, the Port Status returns to Unauthorized.

- **Operational Port Control Direction:** For an unauthorized port, indicates whether the switch controls communication in both directions (preventing reception of incoming frames and transmission of outgoing frames), or just in the incoming direction (preventing reception of incoming frames). The default is Both.
- **Administrative Port Control Direction:** Allows the administrator to set the Operational Port Control Direction to Both or In. The default is Both.
- **Quiet Period:** The number of seconds the switch waits after client authentication fails before trying again. The range is 1 to 65535 seconds. The default is 60 seconds.
- **Transmission Period:** The number of seconds the switch waits for an EAP-Response/Identity frame from the client after sending an EAP-Request/Identity frame during the initial phase of the authentication process. If the switch does not receive a response within this allotted time, it retransmits the EAP-Request/Identity frame. The range is 1 to 65535 seconds. The default is 30 seconds.
- **Supplicant Timeout:** The number of seconds the switch waits for a response from the client (or supplicant) to an EAP-Request. If the switch does not receive a response within this allotted time, it retransmits the EAP-Request frame. The range is 1 to 65535 seconds. The default is 30 seconds.
- **Server Timeout:** The number of seconds the switch waits for a response from the Server during the authentication process. If the switch does not receive a response within this allotted time, it retransmits the EAPOL frame. The range is 1 to 65535 seconds. The default is 30 seconds.
- **Maximum Request:** The maximum number of times the switch retransmits an EAP-Request/Identity frame when it does not receive a response from the client. The range is 1 to 10. The default is 2.
- **Re-auth Period:** The number of minutes between periodic re-authentication of a port. The range is 5 to 1440 minutes. The default is 60 minutes.

- **Re-auth status:** Enables or disables periodic re-authentication of a port. When this parameter is enabled, the switch re-authenticates the client at a periodic interval, as specified by the Re-auth Period parameter. The default is Disabled.

10

Port Mirroring

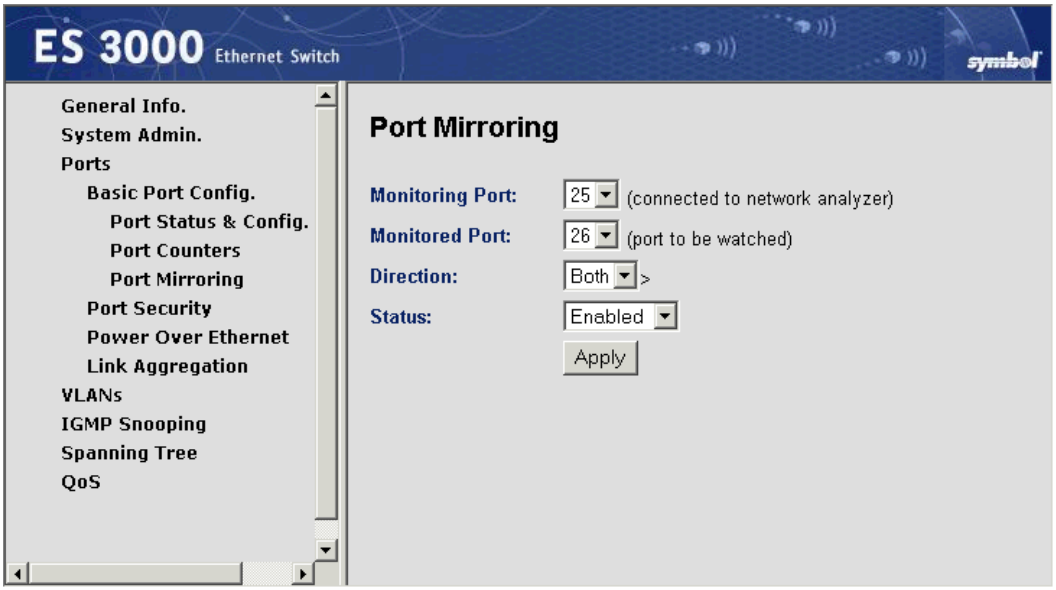
10.1 Port Mirroring Overview

Port mirroring allows one port on the ES3000 to see all of the packets passing through any other port on the switch. Usually, a network analyzer is attached to the monitoring port so the network administrator may debug problems with the monitored port.

The ES3000 has two gigabit Ethernet ports, ports 25 and 26. A 10/100BaseT port would not be able to keep up with the packet flow on a gigabit port. Only another gigabit port may monitor a gigabit port. Any port on the ES3000 may be used to monitor ports 1 through 24, the 10/100BaseT ports.

10.2 Enabling Port Mirroring

To enable port mirroring through the ES3000 web interface, open the *Ports* menu item in the lefthand menu, then open the *Basic Port Config.* item under *Ports*. The *Port Mirroring* menu item will appear under *Basic Port Config.*



Select the monitoring port and the monitored port from the drop down menu of ports. Make sure the monitoring port is not otherwise in use and that it had enough speed to mirror the traffic on the target port.

Monitoring can show all packets, inbound or outbound to the target port, or it can be limited to just one direction. Choose *Direction: RX* to see only inbound packets. Choose *Direction: TX* to see only outbound packets. Choose *Direction: Both* to see all packets, inbound or outbound, to the monitored port.

Finally, set the status to *Enabled* and press the *Apply* button to begin monitoring.

If the monitoring port is a 100/10BaseT port and the monitored port is a gigabit port, the interface will display an error message "Cannot set this port!" To continue, select the link "Return to previous page" and the interface will show the last valid assignment for the port mirroring settings.

10.3 Disabling Port Mirroring

To disable port monitoring, go to the *Port Mirroring* menu item (*Ports > Basic Port Config. > Port Mirroring*) and set the status to *Disabled* and press the *Apply* button. Port mirroring will be disabled.

11

Rate Limiting

11.1 Understanding Rate Limiting

Rate limiting, or *storm control*, prevents ports on the ES3000 switch from being overwhelmed by a DLF, broadcast, or multicast packet storm.

DLF is an abbreviation for Destination Lookup Failure. When a Level 2 Ethernet switch receives a packet for a MAC address which is not yet known to be reachable through particular port, the packet is copied or flooded to all of the ports on the switch (or VLAN).

A storm results when packets overwhelm the LAN, which degrading network performance.

With rate limiting enabled, the switch monitors incoming traffic and counting broadcast packets, multicast packets, and packets for which there has been a destination lookup failure. The switch keeps a separate count of the packets for each type of traffic. When traffic for any one type reaches the threshold, the switch suppresses further traffic of that type until traffic of that type falls below the threshold.

With rate limiting disabled, all traffic is allowed.

11.2 Using Rate Limiting to Control Packet Storms

Use the Storm Control Configuration page (*QoS > Rate Limiting > Broadcast Storm Control*) to enable or disable the different types of storm control and set the packet count threshold.

In the web interface, the administrator can set storm control parameters globally, to apply to all ports. To configure storm control on a port-by-port basis, use the command-line interface.

This page displays the following:

- **DLF:** Unicast (DLF) storm control enabled or disabled. Click the check box for DLF, select Enabled or Disabled from the drop-down list, then click Apply.
- **Broadcast:** Broadcast storm control enabled or disabled. Click the check box for Broadcast, select Enabled or Disabled from the drop-down list, then click Apply.
- **Multicast:** Multicast storm control enabled or disabled. Click the check box for Multicast, select Enabled or Disabled from the drop-down list, then click Apply.
- **Threshold:** The number of packets allowed per second before rate limiting applies. This threshold value applies to all three types of storm control, broadcast, multicast and DLF, though it applies to each seperately. A threshold of 4000 packets per second would allow 3999 broadcast packets a second, 3999 multicast packets a second, and 3999 DLF-handled packets a second without triggering any traffic supression.

The administrator must set a threshold value above 0 before the switch enables storm control for any type of traffic.

12

IGMP Snooping

12.1 Overview of IGMP Snooping

The Internet Group Management Protocol (IGMP) is an Internet protocol that allows an Internet computer (Host) to report its multicast group membership to multicast routers. Multicasting allows one computer on the Internet to send information to other computers that have identified themselves as interested in receiving the information. For further information about IP multicast and IGMP, refer to RFC 1112 and RFC 2236.

The ES3000 switch can "snoop" this messaging protocol to keep track of multicast groups and to insure that multicast traffic is sent only to the appropriate ports within a VLAN.

12.2 Configuring IGMP Snooping

12.2.1 Switch Snooping Configuration

Use the IGMP Snooping Configuration page (*IGMP Snooping* ⇨ *IGMP Snooping Config* ⇨ *IGMP Snooping Config*) to enable or disable IGMP snooping on the switch and set some global snooping parameters. The page displays the following:

- **IGMP Snooping Status:** The global enabled or disabled status of IGMP snooping. The administrator can select Enabled or Disabled. When Enabled, the switch detects IGMP queries, reports, and manages multicast traffic through the switch for all VLANs. When Disabled, the switch forwards traffic and disregards IGMP requests. To filter out snooping on specific VLANs, set the VLAN filter; see "VLAN filtering" on page 3.
- **Host Port Age-Out Time:** The length of time, in seconds, the switch keeps a host in a multicast group without receiving IGMP reports from the host. The value can be within the range 130-1225. The default is 260 seconds.
- **Router Port Age-Out Time:** The length of time, in seconds, the switch keeps router port entries without receiving IGMP queries from the router. Routers usually send protocol advertisements every few seconds. The value can be within the range 60-600. The default is 125 seconds.
- **Report Forward Interval:** The length of time, in seconds, that the switch waits before forwarding an IGMP report to the router from a group from which it has previously sent a report. The value can be within the range 0-25. The default is 5 seconds.
- **Multicast Group Membership table:** The table displays the ports within a VLAN that are associated with a multicast group, which is specified by the Group Mac Address. If a host

has not sent an IGMP report within the Host Port Age-Out time, the port is dropped from the multicast group.

12.2.2 VLAN filtering

Use the VLAN Filter Table page (*IGMP Snooping ⇨ IGMP Snooping Config ⇨ VLAN Filter Table*) to selectively enable or disable IGMP snooping for specific VLANs. The global IGMP snooping status must be enabled for VLAN filtering to take effect, see *Switch Snooping Configuration on page 12-2*.

The display shows a table of which VLANs are filtered out of IGMP snooping.

To control VLAN filtering, type in the ID of the VLAN to control, and select either Filter or Not Filter for the Status parameter. When a VLAN is filtered IGMP snooping does not apply to this VLAN. When the VLAN is not filtered, and global snooping is enabled, the switch snoops for IGMP traffic for the VLAN.

12.2.3 Monitoring the Router Port Table

Use the Router Port Table page (*IGMP Snooping ⇨ IGMP Snooping Config ⇨ Router Port Table*.) to monitor the ports in a VLAN that are sending IGMP reports to the router. The display shows a table of VLAN IDs and the list of ports from that VLAN that are participating in multicast traffic.

Ports are dropped from the list if their connected hosts do not send IGMP reports within the host port age-out time specified on the IGMP Snooping Configuration page. If the router has not sent a IGMP query within the router Port age-out time, the Router Port table is purged.See *Switch Snooping Configuration on page 12-2*.

A

Integrating with the Symbol WS 5000

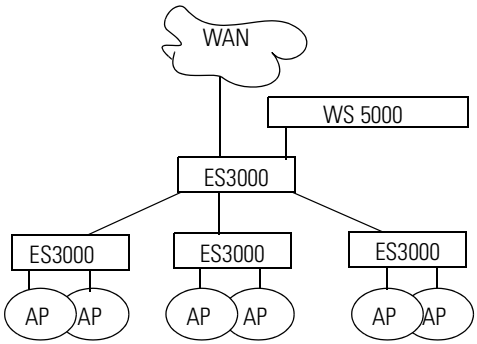
A.1 WS 5000 Overview

The WS 5000 Wireless Switch is an intelligent wireless switch which can take full advantage of Symbol wireless PoE-capable wireless Access Ports. Each WS 5000 can support up to 30 Access Ports. These Access Ports can be segmented into Wireless VLANs with multiple ESSIDs serviced by each Access Port.

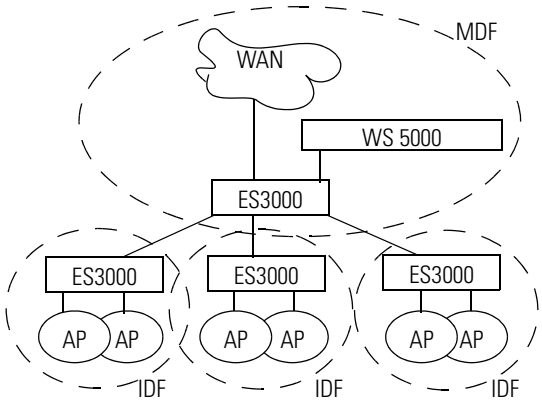
The WS 5000 directly supports four Access Port. Up to 30 Access Ports may be added by connection the WS 5000 to a Layer 2 Ethernet switch, such as the ES3000, and then connecting the Access Ports to the Layer 2 switch.

A.2 Configuring for WS 5000 Integration

The optimal topology for a WS 5000/ES3000 places the ES3000 switches as close to the edge of the network as possible, with the WS 5000 connected directly to an ES3000 near the WAN side of the system. The Access Ports should be on their own VLAN (or multiple VLANs) for optimal performance. Ideally, there should be one VLAN for every ESSID on the WS 5000.

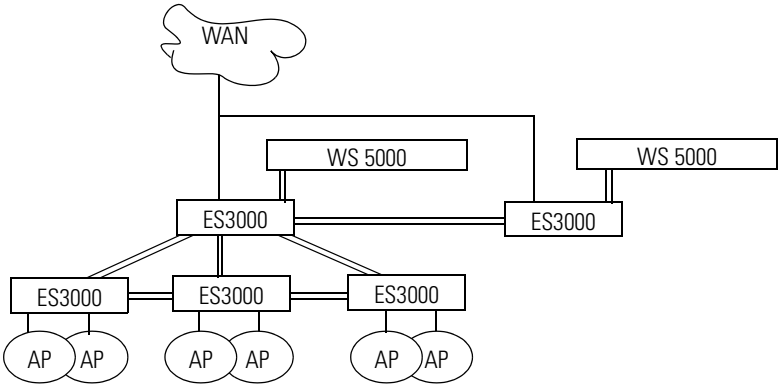


In this topology, the central ES3000, the WS 5000 and the connections to the WAN are called a main distribution frame (MDF) and the edge ES3000 switches and their access ports called an intermediate distribution frame (IDF). Usually the placement of the IDFs will correspond to the physical layout of the building or campus being serviced. There might be one IDF per floor or wing of a building.



The WS 5000 and the Symbol Access Ports do not understand GVRP packets for dynamic VLAN creation, so they should be connected to ports on the ES3000 which are manually configured to be part of the correct VLAN and which are not enabled for GVRP.

If fault-tolerant performance is important, the network should be implemented with multiple connections between the switches and with a backup wireless switch. This network should have use MSTP for spanning tree pruning, there should be no switching devices between the WS 5000 and the Access Ports which do not understand MSTP, and the ES3000 switches, which are closest to the WAN should be configured with the highest spanning tree priority (lowest number) so that they will be chosen as the spanning tree root.



If any of the Access Ports will be supporting any kind of streaming media, most likely VoIP, the WS 5000 and all of the ES3000 switches should be configured with a consistent QoS policy that supports that traffic. See the technical literature of the mobile units for the QoS requirements for that equipment.

B

Customer Support

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone, or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- Serial number of unit
- Model number or product name
- Software type and version number

North American Contacts

Inside North America, contact Symbol by:

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, New York 11742-1300

Telephone: 1-631-738-2400/1-800-SCAN 234

Fax: 1-631-738-5990

Symbol Support Center (for warranty and service information):

telephone: 1-800-653-5350

fax: (631) 563-5410

Email: support@symbol.com

International Contacts

Outside North America, contact Symbol by:

Symbol Technologies
Symbol Place
Winnersh Triangle, Berkshire, RG41 5TP
United Kingdom

0800-328-2424 (Inside UK)
+44 118 945 7529 (Outside UK)

Web Support Sites

MySymbolCare

http://www.symbol.com/services/msc

Symbol Services Homepage

http://symbol.com/services

Symbol Software Updates

http://symbol.com/service/downloads

Symbol Developer Program

http://software.symbol.com/devzone

Additional Information

Obtain additional information by contacting Symbol at:

1-800-722-6234, inside North America

+1-631-738-5200, in/outside North America

http://www.symbol.com/

Glossary

BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DLF	Destination Lookup Failure
DSCP	Differentiated Services Code Points
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
FDB	Forwarding Database
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol

IDF	Intermediate Distribution Frame
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation Protocol
LAN	Local Area Network
MAC	Media Access Control
MDF	Main Distribution Frame
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
NAS	Network Access Server
PD	Powered Device
PoE	Power over Ethernet
PSE	Power Supply Equipment
QOS, QoS	Quality of Service
RADIUS	Remote access Dial-In Service
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
VID	VLAN ID
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WAN	Wide Area Network

Index

O

P

Q

R

S

T

U

V

W

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, New York 11742-1300
http://www.symbol.com

72E-68445-01
Revision A May 2004