DATACOM

DmSwitch Configuration Guide

Revision History

Revision 1.2 2006/08/29

204.4087.02

Contact Information

In order to contact the DATACOM technical support, or sales department:

- Support:
  - E-mail: suporte@datacom-telematica.com.br
  - Phone: +55 51 3358-0122
  - Fax: +55 51 3358-0101
- Sales:
  - E-mail: comercial@datacom-telematica.com.br
  - Phone: +55 51 3358-0100
  - Fax: +55 51 3358-0101
- Internet:
  - www.datacom-telematica.com.br
- Address:
  - DATACOM - Telemática
  - Av. França, 735 - Porto Alegre, RS - Brasil
  - CEP: 90230-220

Table of Contents

List of Tables

List of Figures

List of Examples

Chapter 1. Introduction

1.1. Switch Features

Next table describes the functionabilities of the models of the DmSwitch 3000 series.

Table 1-1. DmSwitch 3000 Models Features

Features	3224F1	3224F2	3324F1	3324F2
Layer 2 Switching	Wire-Speed	Wire-Speed	Wire-Speed	Wire-Speed
Layer 3 Switching	N/A	N/A	Wire-Speed	Wire-Speed
QoS	L2-L7	L2-L7	L2-L7	L2-L7
MPLS	N/A	N/A	L2 VPN over MPLS (Draft Martini)	L2 VPN over MPLS (Draft Martini)
Fast Ethernet Ports	24 x 10/100Base-TX	24 x 10/100Base-TX	24 x 10/100Base-TX	24 x 10/100Base-TX
GBE Ports	4 x ComboGBE (SFP or 10/100/1000Base-T)	4 x ComboGBE (SFP or 10/100/1000Base-T)	4 x ComboGBE (SFP or 10/100/1000Base-T)	4 x ComboGBE (SFP or 10/100/1000Base-T)
Packet Buffer	32 MB	32 MB	32 MB	32 MB
Switch Fabric	12,8 Gbit/s	12,8 Gbit/s	12,8 Gbit/s	12,8 Gbit/s
Flash Memory	16 MB	16 MB	32 MB	32 MB
SDRAM Memory	32 MB	32 MB	64 MB	64 MB
Alarms	N/A	1 output / 3 inputs	N/A	1 output / 3 inputs
Power Supply	Internal AC (100~240V) Power Suply Unit and external RPU connector	Supports 2 AC/DC Full-Range, Hot-Swap Power Suply Units	Internal AC (100~240V) Power Suply Unit and external RPU connector	Supports 2 AC/DC Full-Range, Hot-Swap Power Suply Units

1.2. Software Description

DmSwitch 3000 has many Features. Its default configuration will work for most applications, but they can be configured to best fit the application you want. Next table shows some of the switch's software features.

Table 1-2. Software Features Description

Feature	Details
Auto-negotiation	Speed, duplex mode, flow control e MDI/MDI-X.
Flow Control	Half Duplex: Backpressure; Full Duplex: PAUSE (IEEE 802.3x).
Stackable	Up to 8 switches in a stack. Protection 1:N available. By the management's point of view, all the switches behave as only one switch with more ports. In case of failure, any of the switches in the stack may become the master, ensuring the 1:N protection.
	Hot-Swap - Devices can be inserted to or removed from the stack without the need of restarting.
	Resilient Stack - The stack may be implemented using a redundant connection to guarantee system's stability in case of a link brake up.
	VLAN membership across the stack - VLANS are built using any of the stacking ports.
	Trunking across the stack - A port-channel group may be formed by using ports from different switches of the stack.
	Port Mirror across the stack - Mirroring works between ports of different equipment.
Management	Command Line Interface Cisco like - accessible through SSHv2, Telnet and RS-232.
	SSLv3 Web Server
	SNMP v1/v2c. Implements MIB II (RFC 1213), MIB (RFC 2863) Interface, Ether-Like MIB (RFC 2665, RFC 1643), MIB (RFC 1493) Bridge, MIB (RFC 2674) Extended Bridge and DmSwitch Private MIB.
	RMON, groups 1,2,3 and 9, according with RFC 2819.
	ACLs configuration. Its filter can be built using L2 - L7 levels informations. VLAN inclusion actions, L2 and L3 priority bit writing and packets pass through and discarding.
	SNMP access control filters, Web, Telnet and SSH, making possible to determine which devices will be able to manage the switch.
	Local and Remote Syslog.
	RADIUS (RFC 2865) and TACACS+ users authentication.

Feature	Details
	Network diagnosis tools available: traceroute, ping.
	Cabling Diagnosis Tool - shows the distance of possible cable disruptions and short circuits.
	e-mail notification (SMTP)
	Storage of up to 2 firmware versions in flash memory, with upgrade via TFTP or HTTP/HTTPS.
	Storage of up to 4 different configurations in flash memory, with upload and download via TFTP or HTTP/HTTPS.
	Dinamic or static IP address (DHCP).
	SNTP (RFC 1305, RFC 2030)
VLAN (up to 4096)	VID Tagging (IEEE 802.1Q)
	Port-based VLAN, with possibility of Port Overlap. It means one port can be part of more than one VLAN.
	Protocol-based (IEEE 802.1v), MAC-based, IP-Subnet based.
	Q-in-Q double tagging (IEEE 802.3ac).
	Dynamic VLAN (GVRP)
STP	Classic Spanning Tree (IEEE 802.1D)
	Rapid Spanning Tree (IEEE 802.1w)
QoS	8 buffers on each port.
	Classification and Priorization using TCI tagging (IEEE 802.1p).
	Classification and Priorization using IP Precedence/TOS (RFC 791, RFC 1349).
	Classification and Priorization using DSCP/TOS (RFC 2474), suportando assim DiffServ.
	Classification and Priorization using TCP ports ou UDP ports.
	Rate Shaping (Ingress and Egress), with 64 kbit/s granularity.
	Option between Weighted Round Robin or Strict Priority.
	WRED support.
Port Trunking	32 port-channels, with up to 8 active ports. If more ports are added to the port-channel, they remain in standby.

Feature	Details
	Static or Dinamic Configuration through LACP (IEEE 802.3ad).
Other L2 features	Broadcast Storm Control, with rate configuration on each port.
	Head of Line Blocking protection
	Jumbo Frame support of up to 9KB.
	256 L2 Multicast Groups
	IGMP (v1/v2/v3). Snooping and/or Query functions can be used.
	IEEE 802.1x Port Authentication support.
	Port and Packet Flow Mirrors.

1.3. System Defaults

Next table shows the DmSwitch System's Defaults.

Table 1-3. System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	9600
	Data Bits	8
	Stop Bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username = "admin"
		Password = "admin"
	Normal Exec Level	Username = "guest"
		Password = "guest"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1x Port Authentication	Disabled
CLI Management	Telnet	Enabled
	SSH	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80

Function	Parameter	Default
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	Community Strings	public (read only)
	Traps	Power-On: Enabled
		Link-Up/Link-Down: Enabled
		Authentication: Enabled
		Cold and Warm Start: Enabled
		Configuration change or save: Enabled
		Fan status change: Enabled
		Forbidden access: Enabled
		Login fail and success: Enabled
		SFP presence: Enabled
		Stack attach and detach: Enabled
		Alarm status change: Enabled
		Traps lost: Enabled
	Server	Enabled
Port Configuration	Admin Status	Enabled
	Auto-Negotiation	Enabled
	Flow Control	Disabled
	Port Capability	100BASE-TX: - 10Mbps: Half-Duplex: Enabled - 10Mbps: Full-Duplex: Enabled - 100Mbps: Half-Duplex: Enabled - 100Mbps: Full-Duplex: Enabled - Flow Control (Full-Duplex and Symmetric): Disabled
		1000BASE-T: - 10Mbps: Half-Duplex: Enabled - 10Mbps: Full-Duplex: Enabled - 100Mbps: Half-Duplex: Enabled - 100Mbps: Full-Duplex: Enabled - 1000Mbps: Full-Duplex: Enabled - Flow Control (Full-Duplex and Symmetric): Disabled
Rate Limiting	Input and Output Limits	Disabled
Port Trunking	Static Port-Channel	None

Function	Parameter	Default
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Protocol	Status	Global: Disabled
		Ports: Enabled
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (Global)	Disabled
	GVRP(Port Interface)	Disabled

Chapter 2. General System Configuration

Command Attributes

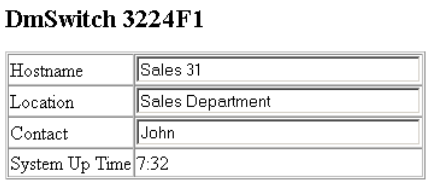
- `Hostname` - Sets the switch's administrative name.
- `Location` - Sets the switch's location name, used for SNMP purposes.
- `Contact` - Sets the switch's contact name, used for SNMP purposes.
- `System Up Time` - The time elapsed from the last reboot.
- `IP Address Mode` - Choose whether the switch will use a static or dynamic IP address for management access through VLAN 1.
- `Gateway IP Address` - Configure a gateway IP address if you want to access this switch from different networks.
- `MAC Address` - The MAC address from the CPU.
- `Reset`- Choose this option to perform a warm reboot.

* *Note: Although the switch can be configured to be accessed by any other set of VLANs, the only one that can use DHCP is the default VLAN 1.*

Configuring System Information via Web

- Open `System - System Information` Fill in a hostname, location and contact information. Use `Apply` to commit.

Figure 2-1. Configuring System Information via Web



Configuring System Information via CLI

- The next example enables the SNTP client, configures the SNTP Polling Interval and the SNTP Server address.

Example 2-1. Configuring System Information via CLI

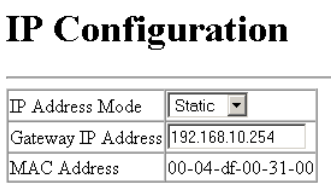
```
DmSwitch3000(config)#hostname Sales31
Sales31(config)#ip snmp-server location Sales Department
Sales31(config)#ip snmp-server contact John
```

```
Sales31(config)#show uptime
19:27:05 up  7:45, load average: 1.21, 1.20, 1.18
Sales31(config)#
```

IP Configuration via Web

- Open `System - IP Configuration` - Select an `IP Address Mode` for VLAN 1 and a `Gateway IP Address`. Click `Apply` to commit.

Figure 2-2. IP Configuration via Web



IP Configuration via CLI

- The next example configures a gateway IP address for the switch, and after changes the configuration to use a DHCP server.

Example 2-2. IP Configuration via CLI

```
DmSwitch3000(config)#ip default-gateway 192.168.10.254
DmSwitch3000(config)#show ip default-gateway
Default gateway: 192.168.10.254

DmSwitch3000(config)#interface vlan 1
DmSwitch3000(config-if-vlan-1)#ip address dhcp
DmSwitch3000(config-if-vlan-1)#
```

- The next example shows how to renew and release with DHCP server.

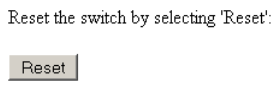
Example 2-3. Renewing and Releasing with DHCP server

```
DmSwitch3000(config-if-vlan-1)#ip address dhcp renew
DmSwitch3000(config-if-vlan-1)#
DmSwitch3000(config-if-vlan-1)#ip address dhcp release
DmSwitch3000(config-if-vlan-1)#
```

Resetting the Switch via Web

- Open `System - Reset` - Click `Reset` and confirm to perform a warm reboot.

Figure 2-3. Resetting the Switch via Web



Resetting the Switch via CLI

- The next example shows how to perform a warm reboot via CLI.

Example 2-4. Resetting the Switch via CLI

```
DmSwitch3000#reboot
System will be restarted, continue <y/N>? y
```

Chapter 3. Managing Firmware and Configuration

This chapter will help you dealing with firmware and storing/transfering configuration.

3.1. Firmware

You can upload firmware from a TFTP server. You can also set the switch to use new firmware without overwriting the previous version.

Command Attributes

- `TFTP Server IP Address` - The IP address of a TFTP server.
- `File Name` - The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for file on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- `Source/Destination Unit` - Specifies the switch stack unit number.
- `Destination/Startup File Name` - Allows specification of filenames already in memory, or the creation of a new filename. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- `Source File Name` - Allows you to specify the name of the chosen source file.

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

3.1.1. Uploading System Software from a TFTP Server

When uploading to switch runtime code from a TFTP server, this file will be stored in a firmware position other than the one used by the running firmware. This new firmware, after a complete upload, will be set as the startup firmware. If some problem occurs during the transfer, the running firmware will stay untouched and will remain as the startup firmware.

> **Note:** Up to two copies of the system software can be stored in the switch. The running system software can not be deleted or overwritten.

- The next example shows how to upload firmware via CLI.

Example 3-1. Uploading System Software from a TFTP Server via CLI.

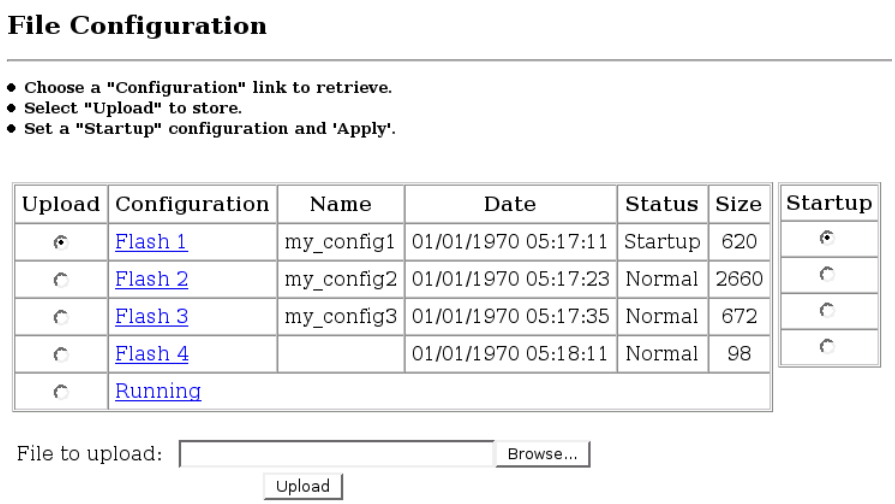
```
DmSwitch3000#copy tftp 192.168.0.1 my_new_firmware.bin firmware
DmSwitch3000#
```

3.2. Configuration

3.2.1. Uploading Configuration Settings

There are 4 memory positions in the switch where configurations can be stored.

Figure 3-1. Managing Configurations via Web.



Uploading a configuration

- Via web, it is possible to upload a configuration to switch by browsing through your files, selecting the upload configuration position and clicking `Upload`.
- The following example shows how to upload a configuration file into flash position 1 via CLI.

Example 3-2. Downloading a configuration via CLI.

```
DmSwitch3000#copy tftp 192.168.0.1 my_new_config.bin flash-config 1
DmSwitch3000#
```

Uploading a configuration and setting it as startup

- Via web, after uploading a configuration to the switch, to set it as startup, you have to mark a startup flash position and click `Apply`.
- The next example show how to upload a configuration to switch via CLI and set it as the startup configuration.

Example 3-3. Via CLI, downloading a configuration and setting it as startup.

```
DmSwitch3000#copy tftp 192.168.0.1 my_new_config.bin startup-config 1
DmSwitch3000#
```

Uploading a configuration and applying it without storing in flash

- Via web, it is possible to upload a configuration to the `Running` position of the switch and it will be applied immediately but not saved.
- The next example shows how to upload a configuration via CLI and apply it without storing in flash.

Example 3-4. Via CLI, downloading a configuration and applying it without storing in flash.

```
DmSwitch3000#copy tftp 192.168.0.1 my_new_config.bin running-config
DmSwitch3000#
```

3.2.2. Copying and Restoring Configuration Settings

Downloading configuration

- Via web, to download a configuration from the switch is as easy as clicking on the corresponding link and selecting the place to save on your computer.
- The next example shows how to dowload a configuration from the switch to a TFTP server by using the CLI.

Example 3-5. Downloading a configuration to a TFTP server.

```
DmSwitch3000#copy flash-config 1 tftp 192.168.0.1 my_flash-config_1.bin
DmSwitch3000#
```

Downloading running configuration

- Via web, this operation is performed by clicking on the `Running` link and selecting the place where to save.
- The following example shows how to download a current configuration from the switch to a TFTP server by using the CLI.

Example 3-6. Downloading a running configuration to a TFTP server.

```
DmSwitch3000#copy running-config tftp 192.168.0.1 my_running-config.bin
DmSwitch3000#
```

Copying a configuration inside the equipment

- The next example shows how to copy a configuration from one position in flash to another via CLI.

Example 3-7. Copying a configuration inside the equipment.

```
DmSwitch3000#copy flash-config 1 flash-config 2
DmSwitch3000#
```

Note: This operation can't be done through the web interface.

Loading a stored configuration

- The next example shows how to load a configuration stored in flash.

Example 3-8. Loading a configuration via CLI.

```
DmSwitch3000#copy flash-config 1 running-config
DmSwitch3000#
```

Note: Via web, this can be done by selecting a startup configuration and rebooting the equipment.

Chapter 4. Port Configuration

4.1. Displaying Port Information

You can use Port Information or Port-Channel Information pages to display the current connection status, including link state, speed/duplex mode, flow control and autonegotiation.

Field Description

- `Port` - Interface number.
- `Name` - Displays interface label.
- `Type` - Indicates the port type.
- `Admin Status` - Displays whether the interface is administratively enabled or not.
- `Oper Status` - Indicates if the link is Up or Down.
- `Speed Duplex Status` - Displays the current speed and duplex status.
- `Flow Control Status` - Indicates the type of flow control currently in use.
- `Autonegotiation` - Displays whether autonegotiation is enabled or not.
- `Port-Channel Member`[1] - Shows if port is a port-channel member.
- `Creation`[2] - Shows if a port-channel is manually configured or dynamically set via LACP.

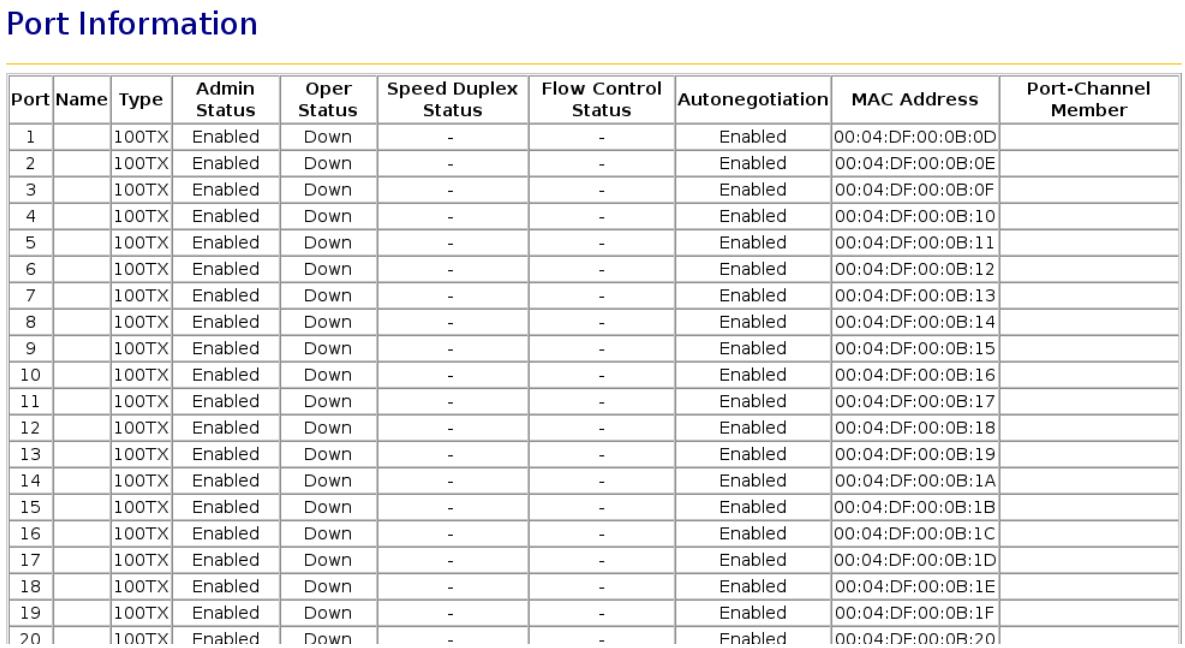
1 Port Information only.

2 Port-Channel Information only.

Displaying Port Information via Web

- Open `Interfaces - Port - Information` or `Interfaces - Port-Channel - Information`

Figure 4-1. Displaying Port Information via Web



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	MAC Address	Port-Channel Member
1		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:0D	
2		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:0E	
3		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:0F	
4		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:10	
5		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:11	
6		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:12	
7		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:13	
8		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:14	
9		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:15	
10		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:16	
11		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:17	
12		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:18	
13		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:19	
14		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:1A	
15		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:1B	
16		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:1C	
17		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:1D	
18		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:1E	
19		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:1F	
20		100TX	Enabled	Down	-	-	Enabled	00:04:DF:00:0B:20	

Displaying Port Information via CLI

- The next example illustrates how to display Port Information via CLI.

Example 4-1. Displaying Port Information via CLI

```
DmSwitch3000#show interfaces status ethernet 1/1
Information of Eth 1/1
 Basic information:
  Port type:              100TX
  MAC address:            00:04:DF:00:31:01
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10M half, 10M full, 100M half, 100M full
  Broadcast storm:        Enabled
  Broadcast storm limit:  500 packets/second
  Flow-control:           Disabled
  LACP:                   Disabled
 Current status:
  Link status:            Up
  Operation speed-duplex: 100M full
  Flow control:           Disabled
DmSwitch3000#
```

4.2. Configuring Interface Connections

You can use the Port Configuration or Port-Channel Configuration page to enable/disable and interface, set autonegotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

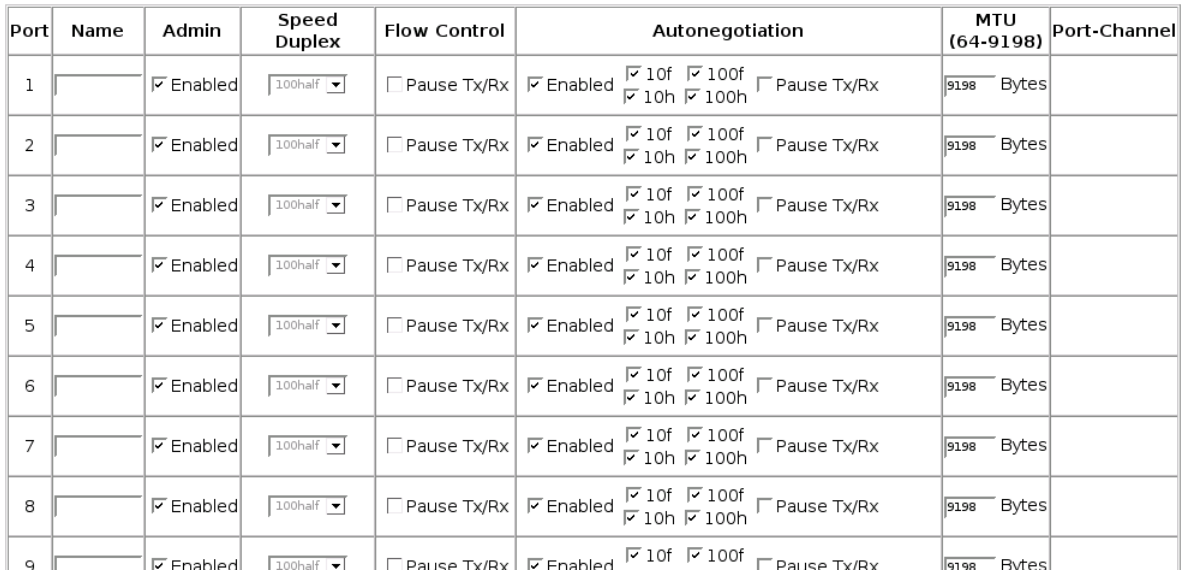
Field Description

- `Name` - Fill in a label for the interface.
- `Admin` - Set the interface's administrative status.
- `Speed Duplex` - Select the speed and duplex configuration. This option is only valid when autonegotiation is disabled.
- `Flow Control` - Set the forced flow control use in the interface. This option is only valid when autonegotiation is disabled.
- `Autonegotiation` - Allows autonegotiation to be enabled or disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When autonegotiation is disabled, you can force the settings for speed, mode, and flow control. The following capabilities are supported.
  - `10half` - Supports 10 Mbps half-duplex operation
  - `10full` - Supports 10 Mbps full-duplex operation
  - `100half` - Supports 100 Mbps half-duplex operation
  - `100full` - Supports 100 Mbps full-duplex operation
  - `1000full` - Supports 1000 Mbps full-duplex operation
  - `flowcontrol` - Supports flowcontrol operation
- `MTU` - Set the maximum transfer unit for the interface. MAC frames with payloads larger than the MTU will be discarded.
- `LACP` - Enables LACP in the interface.
- `Port-Channel` - Indicates if a port is a member of a port-channel.

Port Configuration via Web

- Open `Interfaces - Port - Configuration` or `Interfaces - Port-Channel - Configuration`

Figure 4-2. Port Configuration via Web



Port Configuration

Port	Name	Admin	Speed Duplex	Flow Control	Autonegotiation	MTU (64-9198)	Port-Channel
1		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
2		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
3		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
4		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
5		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
6		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
7		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
8		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f 10h 100h Pause Tx/Rx	9198 Bytes	
9		Enabled	100half	Pause Tx/Rx	Enabled 10f 100f	9198 Bytes	

Port Configuration via CLI

- The next example illustrates how to configure interfaces via CLI.

Example 4-2. Port Configuration via CLI

```
DmSwitch3000(config)#interface ethernet 1/14
DmSwitch3000(config-if-eth-1/14)#description RD

DmSwitch3000(config-if-eth-1/14)#shutdown
DmSwitch3000(config-if-eth-1/14)#no shutdown
DmSwitch3000(config-if-eth-1/14)#no negotiation
DmSwitch3000(config-if-eth-1/14)#speed-duplex 100half
DmSwitch3000(config-if-eth-1/14)#flowcontrol
DmSwitch3000(config-if-eth-1/14)#negotiation
DmSwitch3000(config-if-eth-1/14)#capabilities 100half
DmSwitch3000(config-if-eth-1/14)#capabilities 100full
DmSwitch3000(config-if-eth-1/14)#capabilities flowcontrol
DmSwitch3000(config-if-eth-1/14)#
```

4.3. Port Broadcast Control

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic. Any broadcast packets exceeding the specified threshold will then be dropped.

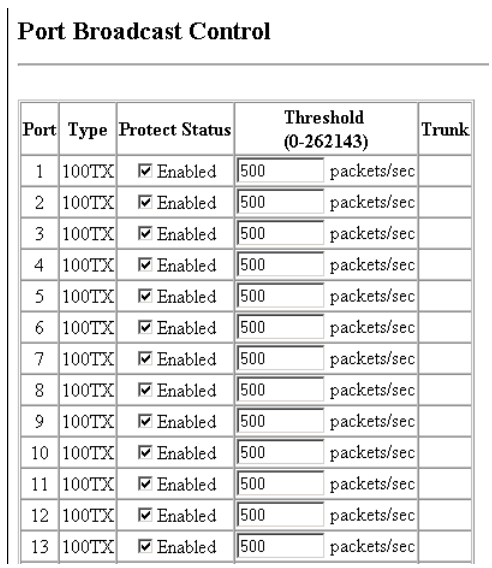
Field Description

- `Port` - Interface number.
- `Type` - Indicates the port type.
- `Protect Status` - Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- `Threshold` - Threshold in packets per second. (Range: 0-262143 packets per second; Default: 500 packets per second)
- `Port-Channel` - Shows if port is configured as a port-channel.

Configuring Port Broadcast Control via Web

- Open `Interfaces - Port - Broadcast Control` or `Interfaces - Port-Channel - Broadcast Control`

Figure 4-3. Configuring Port Broadcast Control via Web



Configuring Port Broadcast Control via CLI

- The next example illustrates how to configure port broadcast control via CLI.

Example 4-3. Configuring Port Broadcast Control via CLI

```
DmSwitch3000(config)#interface ethernet 1/1
DmSwitch3000(config-if-eth-1/1)#no switchport broadcast
DmSwitch3000(config-if-eth-1/1)#exit
DmSwitch3000(config)#interface ethernet 1/2
DmSwitch3000(config-if-eth-1/2)#switchport broadcast packet-rate 600
DmSwitch3000(config-if-eth-1/2)#end
DmSwitch3000#show interfaces switchport ethernet 1/2
Information of Eth 1/2
 Broadcast threshold:           Enabled, 600 packets/second
 MTU:                           9198 bytes
 Ingress rate limit:            Disabled
 Egress rate limit:             Disabled
 Ingress Rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 GVRP status:                   Disabled
 Protocol VLAN:
 Allowed VLAN:                  1(u)
 Forbidden VLAN:
 QinQ mode:                     External
 TPID:                          0x8100
DmSwitch3000#
```

4.4. Configuring Port Monitoring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All monitor sessions have to share the same destination port.
- When monitoring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- `Mirror Sessions` - Displays a list of current mirror sessions.
- `Source Unit` - The unit whose port traffic will be monitored.
- `Source Port` - The port whose traffic will be monitored.
- `Type` - Allows you to select which traffic to mirror to the target port, Rx (receive), or Tx (transmit).
- `Target Unit` - The unit whose port will "duplicate" or "mirror" the traffic on the source port.

- `Target Port` - The port that will "duplicate" or "mirror" the traffic on the source port.

Monitoring a port via CLI

- This example shows how to monitor a port via CLI. Port 10 is specified as the destination where the mirror will be made. Port 12 is the source and tx is the type of traffic to be monitored in this example.

Example 4-4. Monitoring a port via CLI.

```
DmSwitch3000(config)#monitor destination 1/10
DmSwitch3000(config)#interface ethernet 1/12
DmSwitch3000(config-if-eth-1/12)#monitor source tx
DmSwitch3000(config-if-eth-1/12)#
```

4.5. Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on a port. Rate limiting is configured on ports at the edge of a network to limit traffic coming into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or port-channel. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

4.5.1. Rate Limit Configuration

Use the rate limit configuration pages to apply rate limiting.

Command Usage

- Input and output rate limit can be set for individual interfaces.

Command Attribute

- `Port/Port-Channel` - Displays the port number.
- `Rate` - Sets the rate limit in kilobits per second. Must be multiple of 64. (Range: 64-1000000)
- `Burst` - Sets the maximum burst size in kilobits. Must be power of 2. (Range: 32-4096)

Setting the Rate Limit

- This example shows how to set the rate limit via CLI for input and output traffic passing through port 3.

Example 4-5. Setting the Rate Limit via CLI.

```
DmSwitch3000(config)#interface ethernet 1/3
DmSwitch3000(config-if-eth-1/3)#rate-limit input rate 256 burst 128
DmSwitch3000(config-if-eth-1/3)#rate-limit output rate 128 burst 64
DmSwitch3000(config-if-eth-1/3)#
```

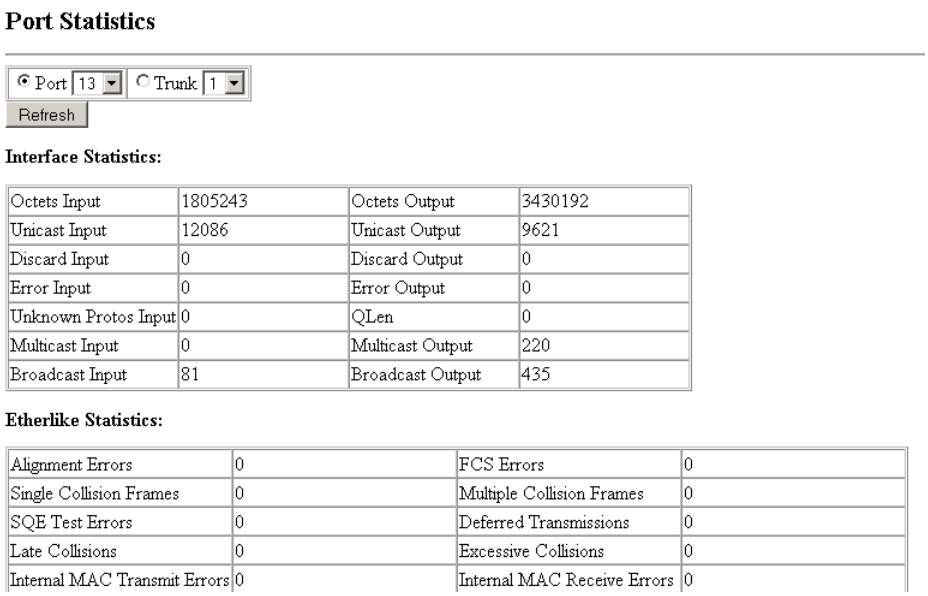
4.6. Displaying Port Statistics

You can display standard statistics on network traffic from the interfaces. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). All values displayed have been accumulated since the last system reboot, and are shown as counts per second.

Displaying Port Statistics via Web

- Open `Port - Port Statistics`.

Figure 4-4. Displaying Port Statistics via Web



Displaying Port Statistics via CLI

- The next example shows detailed port statistics for interface ethernet 13 via CLI.

Example 4-6. Displaying Port Statistics via CLI

```
DmSwitch3000#show interfaces counters ethernet 1/13 detail
Eth 1/13
 Iftable stats:
  Octets input                  : 1823448
  Octets output                 : 3454001
  Unicast input                 : 12257
  Unicast output                : 9764
  Discard input                 : 0
  Discard output                : 0
  Error input                   : 0
  Error output                  : 0
  Unknown protos input          : 0
  QLen                          : 0

 Extended iftable stats:
  Multi-cast input              : 0
  Multi-cast output             : 231
  Broadcast input               : 81
  Broadcast output              : 451

 Ether-like stats:
  Alignment errors              : 0
  FCS errors                    : 0
  Single Collision frames       : 0
  Multiple collision frames     : 0
  SQE Test errors               : 0
  Deferred transmissions        : 0
  Late collisions               : 0
  Excessive collisions          : 0
  Internal mac transmit errors  : 0
  Internal mac receive errors   : 0
  Frame too longs               : 0
  Carrier sense errors          : 3
  Symbol errors                 : 0

 RMON stats:
  Drop events                   : 0
  Octets                        : 5277449
  Packets                       : 22784
  Broadcast packets             : 532
  Multi-cast packets            : 231
  Undersize packets             : 0
  Oversize packets              : 1242
  Fragments                     : 0
  Jabbers                       : 0
  CRC align errors              : 0
  Collisions                    : 0
  Packet size <= 64 octets      : 1129
  Packet size 65 to 127 octets  : 15352
  Packet size 128 to 255 octets : 2283
  Packet size 256 to 511 octets : 1228
  Packet size 512 to 1023 octets: 1071
  Packet size 1024 to 1518 octets: 479
DmSwitch3000#
```

4.7. Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

4.7.1. Setting Static Addresses

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

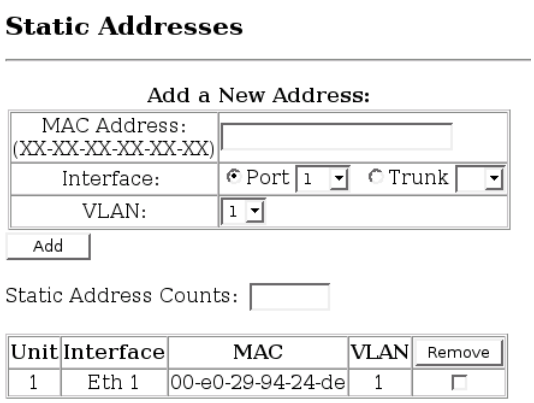
- `Static Address Counts`* - The number of manually configured addresses.
- `Current Static Address Table` - Lists all the static addresses.
- `Interface` - Port or Port-Channel associated with the device assigned a static address.
- `MAC Address` - Physical address of a device maped to this interface.
- `VLAN` - ID of configured VLAN (1-4094).

* Web only.

Displaying Static Addresses via Web

- Open `Address Table - Static Addresses`.

Figure 4-5. Displaying Static Addresses via Web



Adding a static entry to the address table via CLI

- The next example adds an address to the static address table via CLI.

Example 4-7. Adding a static entry to the address table via CLI.

```
DmSwitch3000(config)#mac-address-table static 00-e0-29-94-24-de ethernet 1/1 vlan 1
DmSwitch3000(config)#
```

4.7.2. Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. when the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

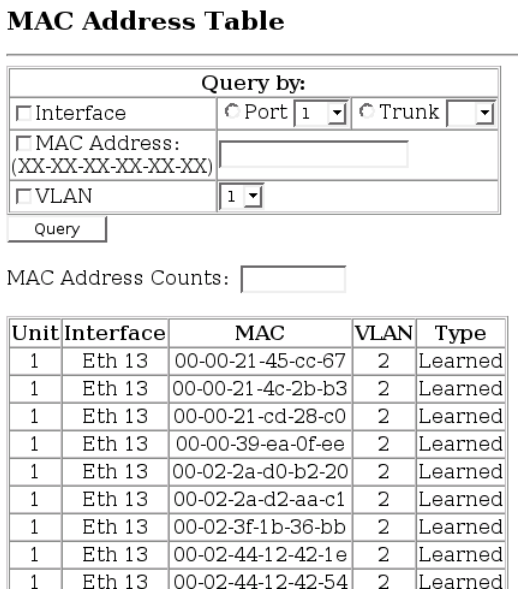
Command Attributes

- `Interface` - Indicates a port or port-channel.
- `MAC Address` - Physical address associated with this interface.
- `VLAN` - ID of configured VLAN (1-4094).
- `Address Table Sort Key` - You can sort the information displayed based on MAC address, VLAN or interface (port or port-channel).

Displaying the Address Table via Web

- Open `Address Table - Address Table`.

Figure 4-6. Displaying Static Addresses via Web



Displaying the Address Table entries for port 1 via CLI

- The next example show how to display the Address Table entries for port 1 via CLI.

Example 4-8. Displaying the Address Table entries for port 1 via CLI.

```
DmSwitch3000#show mac-address-table interface ethernet 1/1
Unit Interface MAC Address       VLAN Type
---- --------- ----------------- ---- ---------
1    Eth  1/ 1 00-e0-29-94-24-de 1    Static
DmSwitch3000#
```

4.7.3. Clearing the Address Table

With the following commands, it is possible to delete entries in the switch MAC Address Table.

Command Attributes

- `Ethernet` - Indicates a ethernet interface where MAC addresses will be deleted.
- `VLAN` - ID of configured VLAN. All its MAC addresses will be deleted.
- `Port-channel` - All MAC address belonging to a port-channel will be deleted.

Deleting MAC Addresses

- This example shows how to delete MAC addresses via CLI. In the example, we delete MAC addresses from Ethernet 12, from VLAN 1, from Port-Channel 3 and then, with the last command, we deleted all MAC addresses registered in the switch.

Example 4-9. Deleting MAC Addresses

```
DmSwitch3000#clear mac-address-table ethernet 1/12
DmSwitch3000#clear mac-address-table vlan 1
DmSwitch3000#clear mac-address-table port-channel 3
DmSwitch3000#clear mac-address-table
DmSwitch3000#
```

4.7.4. Changing Aging Time

You can set the aging time for entries in the dynamic address table.

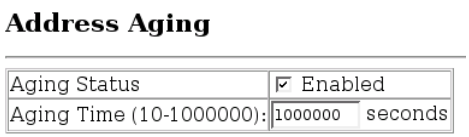
Command Attributes

- `Aging Status` - Enables/disables the function.
- `Aging Time` - The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Setting the Address Aging via Web

- Open `Address Table - Address Aging`.

Figure 4-7. Setting the Address Aging via Web



Setting the Address Aging via CLI

- This example shows how to set Address Aging via CLI.

Example 4-10. Setting the Address Aging via CLI.

```
DmSwitch3000(config)#mac-address-table aging-time 400
DmSwitch3000(config)#
```

4.8. Cable Diagnostics

You can use `cable-diagnostics` command to display the current cable status, including link status, speed, overall status, pair status and pair length.

Field Description

- `Link Status` - Shows if there is a link and the other side is responding.
- `Speed` - Shows link speed if there is a link.
- `Status` - Shows overall status of the cable
- `Pair Status` - Shows pair status.
- `Pair Length` - Shows pair length.

Displaying Cable Diagnostics via CLI

- This example shows how to display cable diagnostics via CLI. First is shown diagnostics for ports 12 and 26 and then is shown part of diagnostics for all ports.

Example 4-11. Displaying Cable Diagnostics via CLI.

```
DmSwitch3000#show cable-diagnostics ethernet 1/12
Port  Link  Speed  Status      Pair  Pair Status  Pair Length
----  ----  -----  ------      ----  -----------  -----------
1/12  Up    100    Ok          A     Ok           10 m (+/- 10 m)
                                 B     Ok           10 m (+/- 10 m)
DmSwitch3000#show cable-diagnostics ethernet 1/26
Port  Link  Speed  Status      Pair  Pair Status  Pair Length
----  ----  -----  ------      ----  -----------  -----------
1/26  Down  N/A    Open        A     Open         0 m
                                 B     Open         0 m
                                 C     Open         0 m
                                 D     Open         1 m
DmSwitch3000#show cable-diagnostics
Port  Link  Speed  Status      Pair  Pair Status  Pair Length
----  ----  -----  ------      ----  -----------  -----------
1/1   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/2   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/3   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/4   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/5   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/6   Up    100    Ok          A     Ok           10 m (+/- 10 m)
                                 B     Ok           10 m (+/- 10 m)
1/7   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/8   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/9   Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
1/10  Down  N/A    Open        A     Open         1 m
                                 B     Open         1 m
...
DmSwitch3000#
```

Observations about cable diagnostics

- If a port is connected to a link partner with a good cable (no short or no open on either pair) and the link partner is not powered up, then the cable status information is valid, but the length information is invalid.
- If a port is connected to a link partner, and if either the link is up or the port is detecting energy from the link partner, then the cable diagnostics result will be unpredictable.

Chapter 5. Stacking

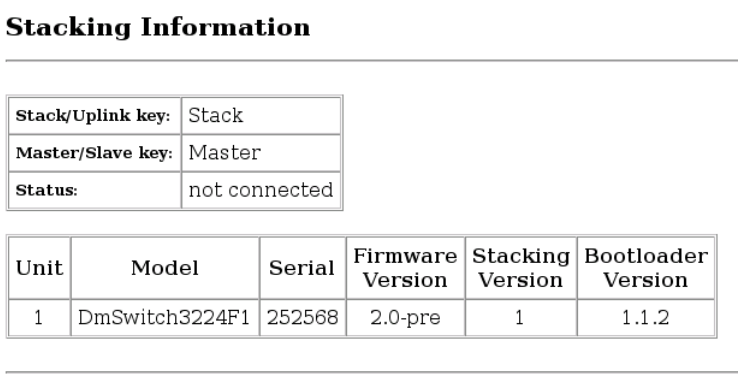
5.1. Displaying Stacking Information

This switch can compond a stack of up to eight switches.

Displaying Stacking Information via Web

- Open `System - Stacking Information`.

Figure 5-1. Displaying Stacking Information via Web



Stacking Information

Stack/Uplink key:	Stack
Master/Slave key:	Master
Status:	not connected

Unit	Model	Serial	Firmware Version	Stacking Version	Bootloader Version
1	DmSwitch3224F1	252568	2.0-pre	1	1.1.2

Displaying Stacking Information via CLI

- The next example show how to display stacking information via CLI.

Example 5-1. Displaying Stacking Information via CLI

```
DmSwitch3000#show stacking

 Stacking information:

  Stack/Uplink key: Stack
  Master/Slave key: Master

  Status:  not connected

                              Firmware        Stacking Bootloader
 Unit Model           Serial Version         Version  Version
 ---- --------------- ------ --------------- -------- ----------
 1    DmSwitch3224F1  252568 2.0-pre         1        1.1.2

DmSwitch3000#
```

Chapter 6. SNTP

The task of manual adjusting and maintaining of internal system clocks in a large or wide spread network of devices can become difficult. In this context, the use of *Simple Network Time Protocol (SNTP)* can be very helpful. SNTP is a simple distributed protocol intended to synchronize clocks of network devices. Using the UDP port 123, a SNTP client contacts a time server and synchronize its clock and date automatically. Remember that the system logs use the configured clock for generating the logs date and time.

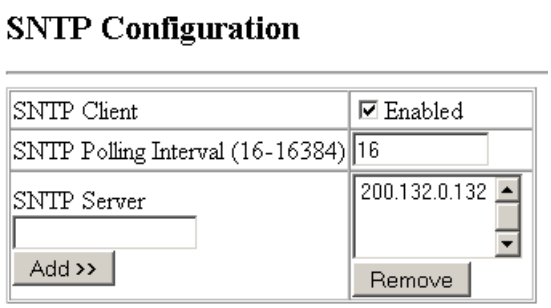
Command Attributes

- `SNTP Client` - Sets the state of the SNTP client.
- `SNTP Polling Interval (16-16384)` - The interval between 2 synchronization polls.
- `SNTP Server` - The IP address of a SNTP server.
- `Current Time` - The time and date currently used by the switch .
- `Time Zone` - Displays the name of time zone used, with the respective time offset.
- `Clock Set` - Use this option when the SNTP client is disabled, to configure a local time and date.
- `Time Zone Set` - Choose this option to configure a time zone and offset for your location.
  - `Name` - the name of your time zone, any string will be accepted. Do not use spaces.
  - `Hours` - offset in hours of your location.
  - `Minutes` - offset in minutes of your location.

Configuring the SNTP Client via Web

- Open `SNTP - Configuration` - Enable/Disable the client, choose a `SNTP Polling Interval` and a `SNTP Server` IP address. Use `Add/Remove/Apply` to commit.

Figure 6-1. Configuring SNTP Client via Web



Configuring SNTP Client via CLI

- The next example enables the SNTP client, configures the SNTP Polling Interval and the SNTP Server address.

Example 6-1. Configuring SNTP Client via CLI

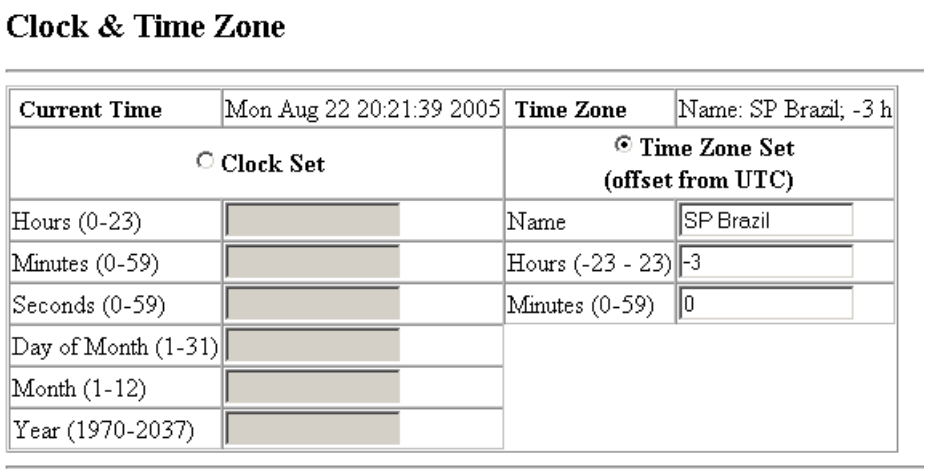
```
DmSwitch3000(config)#sntp client
DmSwitch3000(config)#sntp poll 16
DmSwitch3000(config)#sntp server 200.218.160.160
DmSwitch3000(config)#
```

Configuring the Clock Time Zone via Web

- Open `SNTP - Clock Time Zone` - Select whether using a local `Clock Set` or the `Time Zone Set`. Enter the time information for the option you chose and click `Apply` to commit.

* *Note: When the SNTP client is enabled, the local (`Clock Set`) options will always be overwritten on the next SNTP synchronization polling.*

Figure 6-2. Configuring the Clock Time Zone via Web



Configuring the Clock Time Zone via CLI

- The next example configures a new timezone called "BrazilSP", with time offset of -3 hours and shows the resulting configuration.

Example 6-2. Configuring the Clock Time Zone via CLI

```
DmSwitch3000(config)#clock timezone BrazilSP -3 0
DmSwitch3000(config)#show sntp
  Current time: Mon Aug 22 17:28:48 2005

  SNTP Status: enabled
  SNTP poll interval: 16
  SNTP server 1: 200.218.160.160

  Last successful update: 0 s ago.
    Server used: 200.218.160.160
  Next attempt: in 16 s.
DmSwitch3000(config)#show clock
Mon Aug 22 17:29:26 2005
DmSwitch3000(config)#
```

Chapter 7. System Logs

The embedded syslog agent allows the registering of system events. You can check the event logs in order to debug problems or control user access, for example. Depending on the type of event, it can be saved to the system RAM, flash, sent to a remote log server or destination e-mail address.

Level	*Code*	*Description*
LOG_EMERG	0	kernel panic
LOG_ALERT	1	condition needing immediate attention
LOG_CRIT	2	critical conditions
LOG_ERR	3	errors
LOG_WARNING	4	warning messages
LOG_NOTICE	5	not an error, but may need attention
LOG_INFO	6	informational messages
LOG_DEBUG	7	when debugging a system

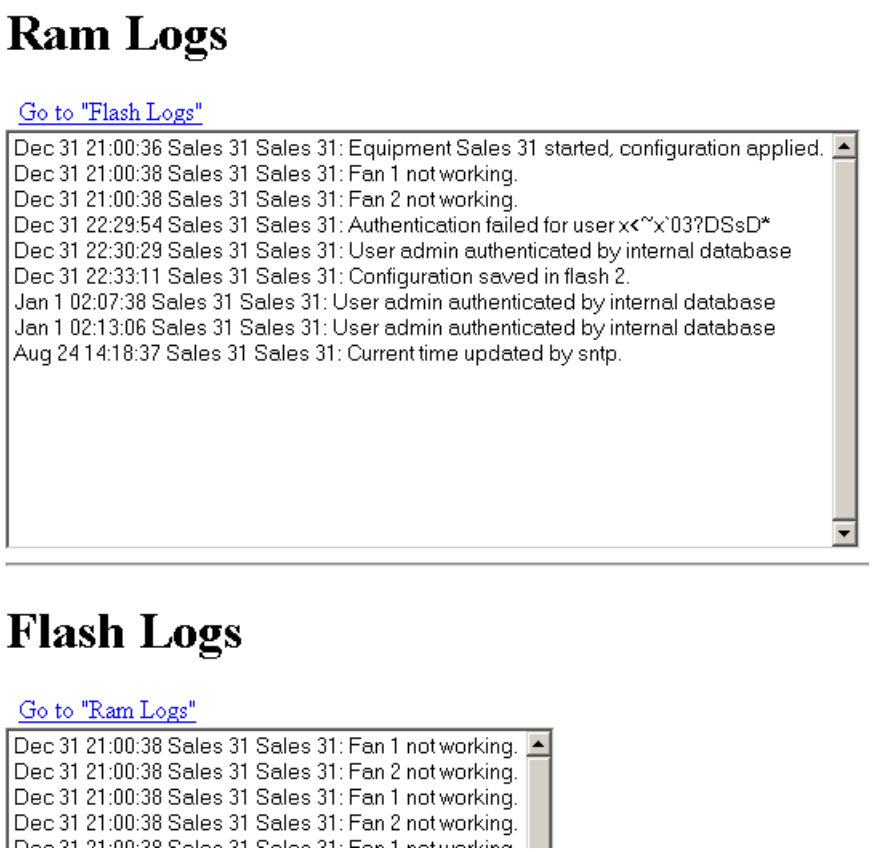
Command Attributes

- `Ram Logs` - Displays the logs saved in RAM.
- `Flash Logs` - Displays the logs saved in flash.
- `System Log Status` - Check `Enabled` to start processing system logs.
- `Flash Level (0-7)` - Sets the range of log severity that will be saved to flash.
- `Ram Level (0-7)` - Sets the range of log severity that will be saved to RAM.
- `Remote Log Status` - Check `Enabled` to enable the sending of logs to a remote log server.
- `Remote Facility (16-23)` - Sets the remote facility type.
- `Remote Level (0-7)` - Sets the range of log severity that will be sent to the remote log server.
- `SMTP Status` - Check `Enabled` to enable the sending of log messages by e-mail.
- `SMTP Level (0-7)` - Sets the range of log severity that will be sent to the destination e-mail.
- `Source e-mail` - Sets the source e-mail address inserted in messages.
- `Destination e-mail` - Sets the destination e-mail address.
- `SMTP Servers` - Sets a new SMTP server IP address.

Displaying System Logs via Web

- Open `System - Log - Logs`.

Figure 7-1. Displaying System Logs via Web



Displaying System Logs via CLI

- The next example shows the logs from RAM and flash.

Example 7-1. Displaying System Logs via CLI

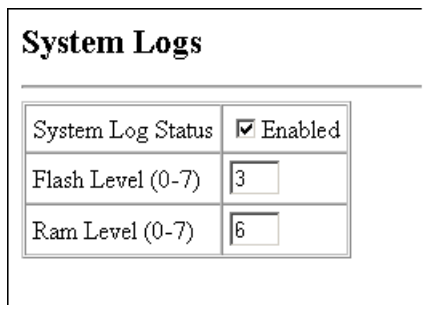
```
DmSwitch3000#show log ram
Dec 31 21:00:36 DmSwitch3000 : Equipment DmSwitch3000 started, configuration applied.
Dec 31 21:00:38 DmSwitch3000 : Fan 1 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 2 not working.
Dec 31 22:29:54 DmSwitch3000 : Authentication failed for user x<~x‘03?DSsD*
Dec 31 22:30:29 DmSwitch3000 : User admin authenticated by internal database
Dec 31 22:33:11 DmSwitch3000 : Configuration saved in flash 2.
Jan  1 02:07:38 DmSwitch3000 : User admin authenticated by internal database
Jan  1 02:13:06 DmSwitch3000 : User admin authenticated by internal database
Aug 24 14:18:37 DmSwitch3000 : Current time updated by sntp.
Aug 24 15:39:42 DmSwitch3000 : User admin authenticated by internal database
DmSwitch3000#show log flash
Dec 31 21:00:38 DmSwitch3000 : Fan 1 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 2 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 1 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 2 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 1 not working.
```

```
Dec 31 21:00:38 DmSwitch3000 : Fan 2 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 1 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 2 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 1 not working.
Dec 31 21:00:38 DmSwitch3000 : Fan 2 not working.
DmSwitch3000#
```

Configuring System Logs via Web

- Open `System - Log - System Logs` - Check `Enabled` to start processing system logs, choose the range of log severity that will be saved to flash and RAM. Click `Apply` to commit.

Figure 7-2. Configuring System Logs via Web



Configuring System Logs via CLI

- The next example enables the logging of events, sets the range to be saved in RAM from 0 to 6 and in flash from 0 to 3.

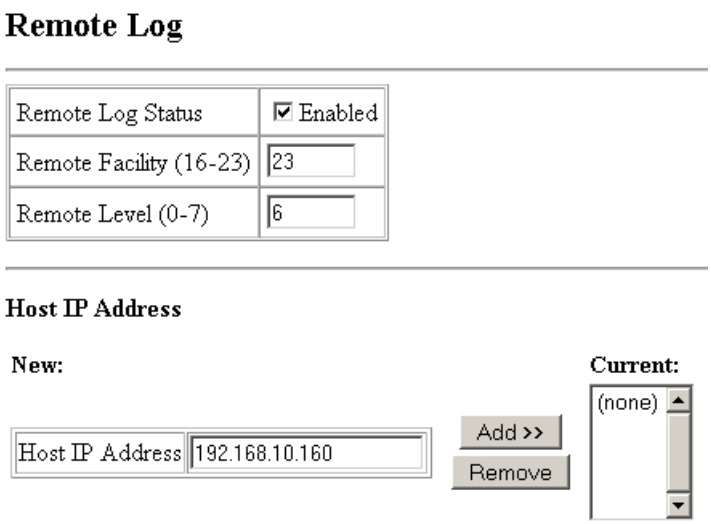
Example 7-2. IP Configuration via CLI

```
DmSwitch3000(config)#logging on
DmSwitch3000(config)#logging history ram 6
DmSwitch3000(config)#logging history flash 3
DmSwitch3000(config)#show logging ram
               Syslog logging: Enabled
       History logging in RAM: info (6)
DmSwitch3000(config)#show logging flash
               Syslog logging: Enabled
     History logging in flash: error (3)
DmSwitch3000(config)#show logging sendmail
               Syslog logging: Enabled
               SMTPLOG status: Enabled
          SMTPLOG level type: warn (4)
         SMTPLOG source email: dmswitch@sales.com
    SMTPLOG destination email: manager@sales.com
    SMTPLOG server IP address: 192.168.10.1
```

Configuring Remote Logs via Web

- Open `System - Log - Remote Logs` - Check `Enabled` to enable remote logging, choose the remote facility type, range of log severity that will be sent to the remote log server and enter the server's IP address. Click `Apply` to commit.

Figure 7-3. Configuring Remote Logs via Web



Configuring Remote Logs via CLI

- The next example enables the use of remote logging, defines a server IP address, facility type and range of log severity that will be sent to the remote log server from 0 to 6.

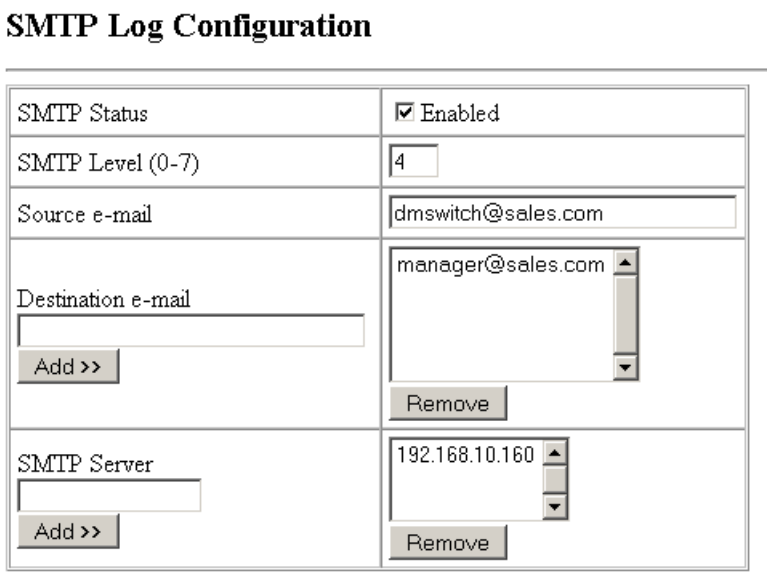
Example 7-3. Resetting the Switch via CLI

```
DmSwitch3000(config)#logging trap 6
DmSwitch3000(config)#logging host 192.168.10.160
DmSwitch3000(config)#logging facility 23
DmSwitch3000(config)#sh logging trap
                     Syslog logging: Enabled
                   REMOTELOG status: Enabled
             REMOTELOG facility type: 23
                REMOTELOG level type: info (6)
         REMOTELOG server IP address: 192.168.10.160
DmSwitch3000(config)#
```

Configuring SMTP Logs via Web

- Open `System - Log - SMTP Configuration` - Check `Enabled` to enable SMTP logging, choose the range of log severity that will be sent by SMTP, enter the source and destination e-mail. Set a SMTP server IP address and click `Apply` to commit.

Figure 7-4. Configuring SMTP Logs via Web



Configuring SMTP Logs via CLI

- The next example enables the use of SMTP logging, defines a SMTP server IP address, source and destination e-mail and range of log severity that will be sent to destination by e-mail.

Example 7-4. Configuring SMTP Logs via CLI

```
DmSwitch3000(config)#logging sendmail
DmSwitch3000(config)#logging sendmail level 4
DmSwitch3000(config)#logging sendmail source-email dmswitch@sales.com
DmSwitch3000(config)#logging sendmail destination-email manager@sales.com
DmSwitch3000(config)#logging sendmail host 192.168.10.1
DmSwitch3000(config)#show logging sendmail
               Syslog logging: Enabled
               SMTPLOG status: Enabled
          SMTPLOG level type: warn (4)
         SMTPLOG source email: dmswitch@sales.com
    SMTPLOG destination email: manager@sales.com
    SMTPLOG server IP address: 192.168.10.1
DmSwitch3000(config)#
```

Chapter 8. Managing Security

Security is a very important issue in networks. This switch has a complete set of features that allows you to improve the security of your network:

- *Local User Management:* This switch maintains a local user database so a user can be authenticated locally on the switch.
- *Remote User Authentication*: An user can be authenticated using a *Remote Authentication Dial-in User Service (RADIUS)* or *Terminal Access Controller Access Control System Plus (TACACS+)* server.
- *Secure Web Access*: By using the *Secure Hypertext Transfer Protocol (HTTPS)*, a secure encrypted session is established between a manager and the switch.
- *Secure Shell*: The *Secure Shell (SSH)* is a protocol that provides encrypted connections to a remote host. The use of this protocol allows to establish a secure connection between your host computer and this switch.
- *Secure Network Access*: By implementing the IEEE 802.1x port authentication this switch allows to restrict the access to the network for authorized users only.
- *Management Restricted Access*: A network filter can be configured in order to avoid access to management interfaces from any undesired network IP address.

This switch supports the following Security Features:

- Local User Management
- RADIUS authentication
- TACACS+ authentication
- HTTPS server
- SSH access
- IEEE 802.1x
- Management IP Filter

8.1. Local User Management

By using this option a user can be authenticated locally on the switch. Due to its easier configuration, this feature is often used when few users need access to the switch management interface.

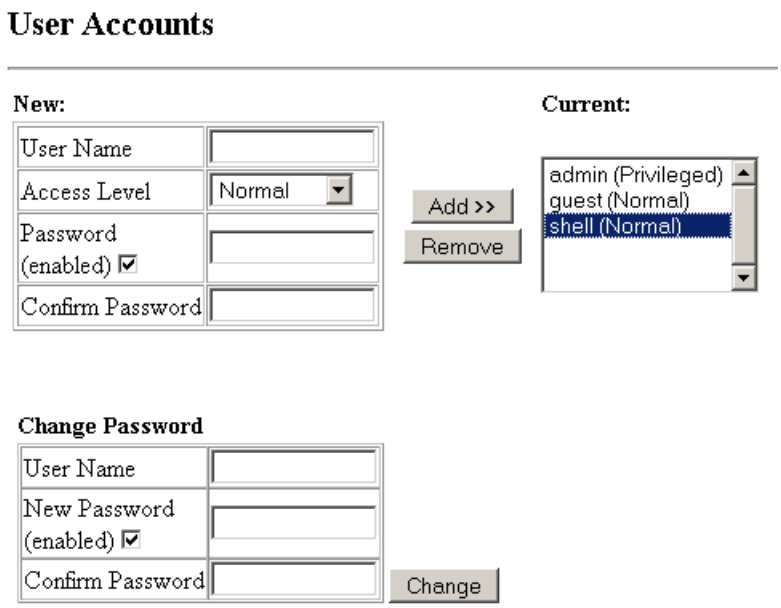
Command Attributes

- `User Name` - A unique text string that identifies the user (Case Sensitive).
- `Access Level` - Choose whether the user will be given a normal or privileged mode.
- `Password` - Enter the password for this user (Case Sensitive).
- `Enabled` - By enabling this option a password will always be required for this user.

Configuring Local User Accounts via Web

- Open `Security - User Accounts` - Enter a `User Name`, `Access Level` and a `Password` (or choose an already existing user to change or remove some property) . Use `Add/Remove/Change` to commit.

Figure 8-1. Configuring Local User Accounts via Web



Configuring Local User Accounts via CLI

- The next example creates a new privileged user "John" with password "S19ma_p!", and removes a normal user.

Example 8-1. Configuring Local User Accounts via CLI

```
DmSwitch3000(config)#username John access-level 15
DmSwitch3000(config)#username John password 0 S19ma_p!
DmSwitch3000(config)#no username Peter
DmSwitch3000#show running-config
Building configuration...
!
terminal timeout 0
!
username admin access-level 15
username admin password 7
username guest access-level 0
username guest password 7
username shell access-level 0
username shell nopassword
username John access-level 15
username John password 7
```

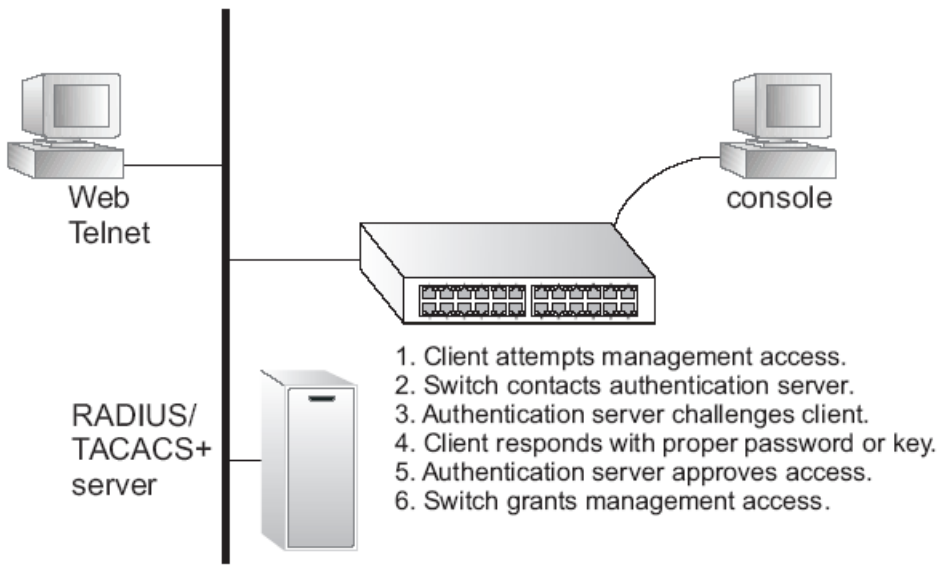
```
DmSwitch3000#
```

Note: The use of strong passwords is highly recommended. In order to create a strong password you have to use strings that are a combination of letters, numbers and symbols (@, #, $, %, etc.). Passwords are case-sensitive, a strong password should contain letters in both uppercase and lowercase. Strong passwords do not contain words found in a dictionary.

8.2. Authentication Settings

This switch allows you to configure multiple authentication methods in order to improve security, availability and scalability. By default, the local users database is used to configure access rights. You can also use a remote authentication server using RADIUS or TACACS+ protocols to execute the authentication task. A remote authentication server maintains a database with authorized usernames and passwords and is accessed by the switch when an user tries to log in to the switch's management interface (via Web access, SSH, Telnet and console port).

Figure 8-2. Using Remote Authentication Servers



You can also configure multiple authentication servers in order to increase availability in case of server failure. The servers will be contacted by the switch in the same order specified by the configuration parameters. You can choose up to three different methods (Local, RADIUS and TACACS+).

Command Attributes

- `Login` - Choose the order of searching for users. The Local option will only be skipped when a username entered is not present in the local database. RADIUS and TACACS+ options will only be skipped when the respective servers are down.

* *(Note that an ACCESS REJECT message received from a authentication server does not generate a skip action and will always result in authentication denial)*

.

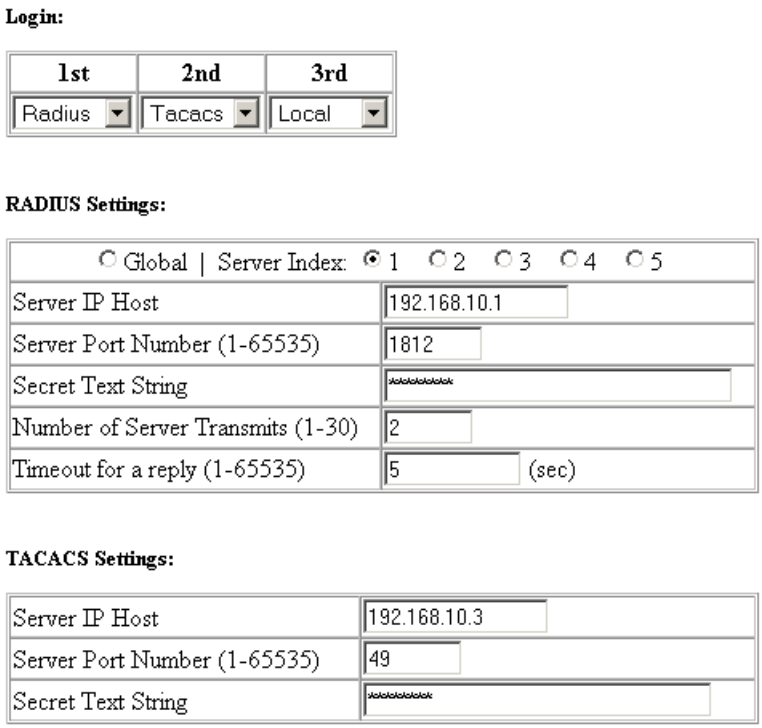
- `RADIUS Settings` - Options used when RADIUS authentication takes place.
  - `Global` - Global RADIUS options.
  - `ServerIndex` - This server index is used in the server search order. The authentication process stops with a ACCESS ACCEPT or ACCESS REJECT response.
  - `Server IP Host` - Specify an IP address from a RADIUS server.
  - `Server Port Number (1-65535)` - Specify the port number which the RADIUS server will be contacted. The default RADIUS server service port number is UDP 1812.
  - `Secret Text String` - Messages exchanged between the switch and RADIUS server are authenticated through the use of this secret text string.
  - `Number of Server Transmits (1-30)` - Number of times the switch will try to authenticate before proceeding to the next server.
  - `Timeout for a reply (1-65535)` - The time interval the switch waits for a response from the RADIUS server without sending another request.

- `TACACS Settings` - Options used when TACACS+ authentication takes place.
  - `Server IP Host` - Specify an IP address from a TACACS+ server.
  - `Server Port Number (1-65535)` - Specify the port number which the TACACS+ server will be contacted. The default TACACS+ server service port number is TCP 49.
  - `Secret Text String` - Messages exchanged between the switch and TACACS+ server are authenticated through the use of this secret text string.

Configuring Authentication Settings via Web

- Open `Security - Authentication Settings` - Select the login search order and the settings for each protocol selected. Click `Apply` to commit.

Figure 8-3. Configuring Authentication Settings via Web



Configuring Authentication Settings via CLI

- The next example demonstrates how to select an authentication method, configure two different RADIUS servers (for fail-over purposes) and a TACACS+ server.

Example 8-2. Configuring Authentication Settings via CLI

```
DmSwitch3000(config)#authentication login radius tacacs local
DmSwitch3000(config)#radius-server host 1 address 192.168.10.1
DmSwitch3000(config)#radius-server host 1 port 1812
DmSwitch3000(config)#radius-server host 1 key secret1
DmSwitch3000(config)#radius-server host 2 address 192.168.10.2
DmSwitch3000(config)#radius-server host 2 port 1812
DmSwitch3000(config)#radius-server host 2 key secret2
DmSwitch3000(config)#tacacs-server host 192.168.10.3
DmSwitch3000(config)#tacacs-server port 49
DmSwitch3000(config)#tacacs-server key secret3
DmSwitch3000(config)#exit
DmSwitch3000#show radius-server
RADIUS authentication configuration:
  Default Key:   ********
  Default Port:  1812
  Timeout:       5
  Retries:       2
  Host 1:
```

```
    Address:     192.168.10.1
    Port:        1812
    Key:         ********
  Host 2:
    Address:     192.168.10.2
    Port:        1812
    Key:         ********
  Host 3:
  Host 4:
  Host 5:
DmSwitch3000#show tacacs-server
TACACS authentication configuration:
  Server: 192.168.10.3
  Key:    ********
  Port:   49
DmSwitch3000#
```

8.3. HTTP and HTTPS Configuration

The HTTPS server embedded in this switch allows the establishment of a secure encrypted web connection between an authenticated (privileged) manager and the switch's web configuration interface. Both the secure HTTPS and the conventional HTTP server can be used simultaneously, in order to access the secure interface use `https://switch[:port_number]` instead of `http://switch` in your web browser. Note that when an encrypted connection is established a locked padlock should appear in your web browser bar. The web browsers recommended for use with the web interface are Internet Explorer 6.x or above and Mozilla Firefox 1.03 and above.

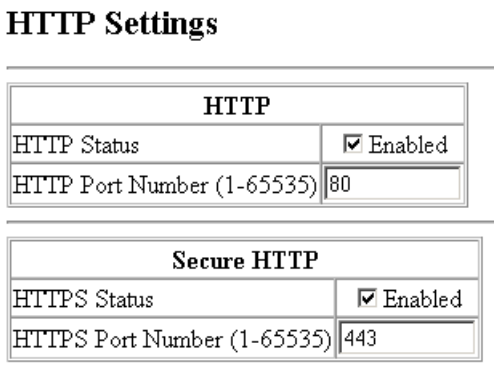
Command Attributes

- `HTTP Status` - Choose whether the web server will be enabled or not.
- `HTTP Port Number (1-65535)` - Enter a valid port number or leave the default value. (Default: 80)
- `HTTPS Status` - Choose weather the secure web server will be enabled or not.
- `HTTPS Port Number (1-65535)` - Enter a valid port number or leave the default value. (Default: 443)
- `HTTP and HTTPS Connections Maximum Number (1-32)` - Enter a limit number of possible simultaneous connections. (Default: 8)

Configuring HTTP and HTTPS via Web

- Open `Security - HTTP Settings` - select the desired server status and port number. Use `Apply` to commit.

Figure 8-4. Configuring HTTP and HTTPS via Web



Configuring HTTP and HTTPS via CLI

- The next example enables the HTTP and HTTPS servers using port numbers 80 and 443 respectively. It also limits the number of possible simultaneous connections in 8.

Example 8-3. Configuring HTTP and HTTPS via CLI

```
DmSwitch3000(config)#ip http server
DmSwitch3000(config)#ip http port 80
DmSwitch3000(config)#ip http secure-server
DmSwitch3000(config)#ip http secure-port 443
DmSwitch3000(config)#ip http max-connections 8
DmSwitch3000(config)#
```

8.3.1. Replacing the Secure Certificate

The replacement of the default SSL Secure Certificate is highly recommended for security reasons. In order to replace this certificate you must generate or obtain an unique certificate (preferably from a recognized certification authority), private key and password and save them in a tftp server.

Replacing the Secure Certificate via CLI

- The next example shows how to replace the default secure certificate by the new certificate file "CertificateFileName" with the private key file "PrivateKeyFileName" and password "passwd" from a TFTP server 192.168.10.160. Note that the switch must be rebooted in order to the new certificate become available.

Example 8-4. Replacing the Secure Certificate via CLI

```
DmSwitch3000(config)#fetch tftp https-certificate 192.168.10.160
CertificateFileName PrivateKeyFileName passwd
DmSwitch3000(config)#exit
DmSwitch3000#reboot
```

8.4. Configuring the Secure Shell - SSH

The Secure Shell (SSH) is a protocol designed for logging into and executing commands on a remote network host.The SSH protocol can be considered a secure alternative to telnet because its connections are encrypted. Due to its higher security, you should consider the use of SSH instead of telnet whenever possible.

This switch has an embedded SSH server that allows you to remotely log in and execute commands (just like a telnet connection, but in a secure way). It is also possible to log in using a public/private key mechanism instead of entering an user and password.

* *Note: In order to use the SSH remote login you will need first to generate a public key.*

8.4.1. SSH Server Settings

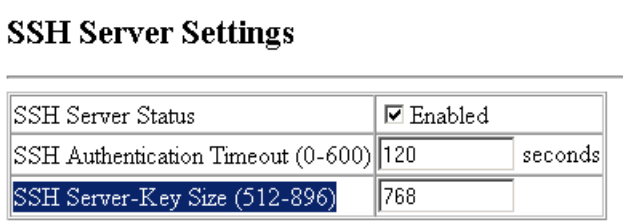
Command Attributes

- `SSH Server Status` - Choose whether the SSH server will be enabled or not.
- `SSH Authentication Timeout (0-600)` - The amount of time in seconds the SSH server will wait for a response from a client during authentication. (Default: 120 seconds)
- `SSH Server-Key Size (512-896)`[- Specifies the SSH server key size. (Range: 512-896 bits). Server key is a private key that is never shared outside the switch. Host key is shared with the SSH client, and is fixed at 1024 bits.]
- `SSH Connections Maximum Number (1-32)` - Enter a limit number of possible simultaneous connections. (Default: 8)

Configuring SSH Server Settings via Web

- Open `Security - SSH - Settings` - select the desired server status, authentication timeout and server key size . Use `Apply` to commit.

Figure 8-5. Configuring SSH Server Settings via Web



Configuring SSH Server Settings via CLI

- The next example enables the SSH server using a timeout of 120 seconds and server key size of 768 bits. It also limits the number of possible simultaneous connections in 8.

Example 8-5. Configuring SSH Server Settings via CLI

```
DmSwitch3000(config)#ip ssh server
DmSwitch3000(config)#ip ssh server timeout 120
DmSwitch3000(config)#ip ssh server-key size 768
DmSwitch3000(config)#ip ssh max-connections 8
DmSwitch3000(config)#
```

8.4.2. SSH Host-Key Settings

Command Attributes

- `Public-Key of Host-Key` - A 512 bits value that will be used by the client in order to establish an encrypted terminal connection to the switch's SSH server.
  - `RSA` - Hexadecimal RSA fingerprint value.
  - `DSA` - Hexadecimal DSA fingerprint value.

Configuring SSH Host-Key Settings via Web

- Open `Security - SSH - Host-Key Settings` - select the desired key type to be generated or deleted (RSA for SSH 1, DSA for SSH 2, or Both). Use `Generate` or `Clear` to commit.

* *Note: Depending on the internal CPU workload, the key generation process may take several minutes to finish.*

Figure 8-6. Configuring SSH Host-Key Settings via Web

Configuring SSH Host-Key Settings via CLI

- The next example generates a RSA key and deletes a previous DSA key. It also fetches from the tftp server 192.168.10.160 and enables the SSH server using a timeout of 120 seconds and server key size of 768 bits.

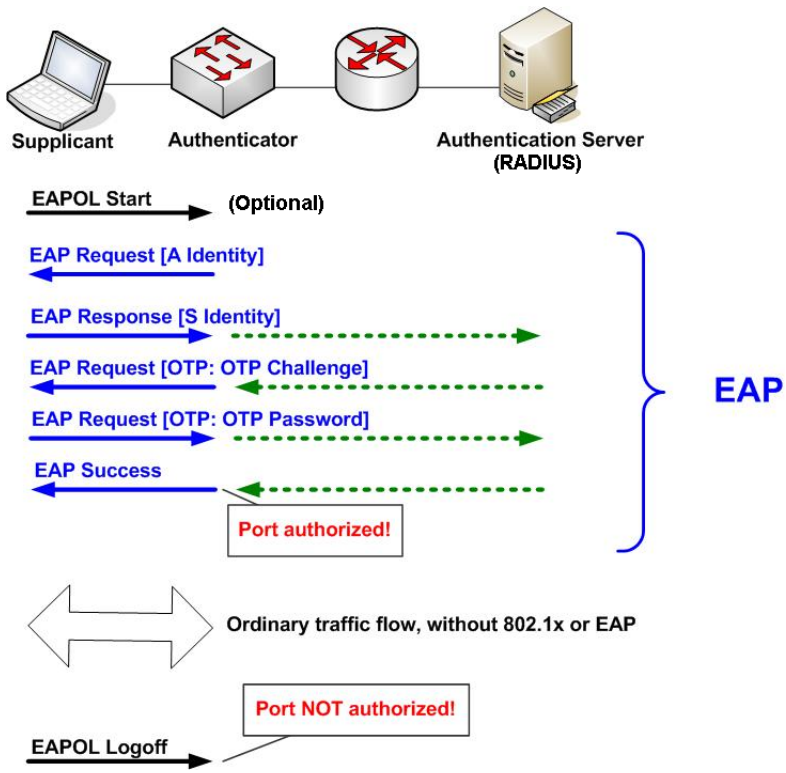
Example 8-6. Configuring SSH Host-Key Settings via CLI

```
DmSwitch3000(config)#ip ssh host-key generate rsa
DmSwitch3000(config)#ip ssh host-key clear dsa
DmSwitch3000(config)#fetch tftp public-key 192.168.10.160 File User
```

8.5. Configuring Port Authentication with 802.1x

Local Area Networks, as defined by the IEEE Standard 802.1D in 1998, allow access to unauthorized users and devices which are able to be connected physically to the network. In this context, the possibility of restricting access to the network becomes an important issue. The IEEE 802.1x standard establishes a port security mechanism that grants access only to authenticated users and devices.

Figure 8-7. 802.1x Success Authentication Message Exchange



The 802.1x authentication framework works like this:

- The *Supplicant* (client user or device) wishes to access the network, so it sends an *Extensible Authentication Protocol Over LAN (EAPOL)* Start message to the *Authenticator* (the switch).
- The authenticator receives the EAPOL Start message and then sends an *Extensible Authentication Protocol (EAP)* Request to the client, requesting its identity. It is also possible that the authenticator itself detects the presence of a client and then it will send the same EAP request.
- The supplicant replies with its identity.
- The supplicant's identity is then forwarded using an EAP message to the authentication server (usually a RADIUS server).
- The authentication server challenges the supplicant.
- The supplicant replies with its credentials.
- If the credentials are approved by the server, access is granted to the supplicant.
- The supplicant is allowed to send and receive traffic normally.
- When the supplicant wishes to disconnect from the network, it sends an EAPOL Logoff message.

* *Note: All the EAP message exchange is done between the switch and the client or the switch and the authentication server. For security reasons no direct communication between the supplicant and authentication server is allowed.*

In order to implement 802.1x port security in your network you should first check the following items:

- The switch must be configured with an IP address and optionally with a network gateway.
- At least one RADIUS server must be configured in the `Security - Authentication Settings` page.
- Each client must have a properly configured supplicant 802.1x software in order to the authentication take place.
- The RADIUS server and clients must support the EAP authentication type MD5.

8.5.1. 802.1x Port Configuration

Command Attributes

- `802.1x System Authentication Control` - Choose whether the 802.1x System Authentication Control will be enabled or not. (Default: Disabled)
- `Port` - Port number.
- `Mode` - Sets the authentication mode:
  - `Auto` - Only 802.1x clients will be authorized by the authentication server. Non-802.1x clients will not be able access the network.
  - `Force-Authorized` - All clients (either 802.1x or not) will access the network. (This is the default setting.)
  - `Force-Unauthorized` - No client will be able to access the network.

- `Authorized` - Displays whether the connected client status is authorized (`Yes`) or not (`No`).
- `Re-authen` - Choose if re-authentication will took place every `Re-authen Period`. Use this option to force the switch to check periodically the authenticity of the client. (Default: Disabled)
- `Max-Req (1-10)` - Sets the maximum EAP request messages transmitted by the switch before terminating an authentication session. (Default 2)
- `Quiet Period (1-65535)` -The period of time (in seconds) the switch waits before starting a new authentication session after a Max-Req count has been exceeded. (Default: 60 seconds)
- `Re-authen Period (1-65535)` -The time interval (in seconds) the switch waits before trying to re-authenticate the client. (Default 3600 seconds)
- `TX Period (1-65535)` - The time interval (in seconds) the switch waits before re-transmitting an EAP packet. (Default 30 seconds)
- `Supplicant` - The MAC address of the authenticated client.
- `Port-Channel` - Displays the port-channel index when the port is a port-channel member.
- `Uptime*` - Displays the time interval passed from the last authentication. (*CLI only)

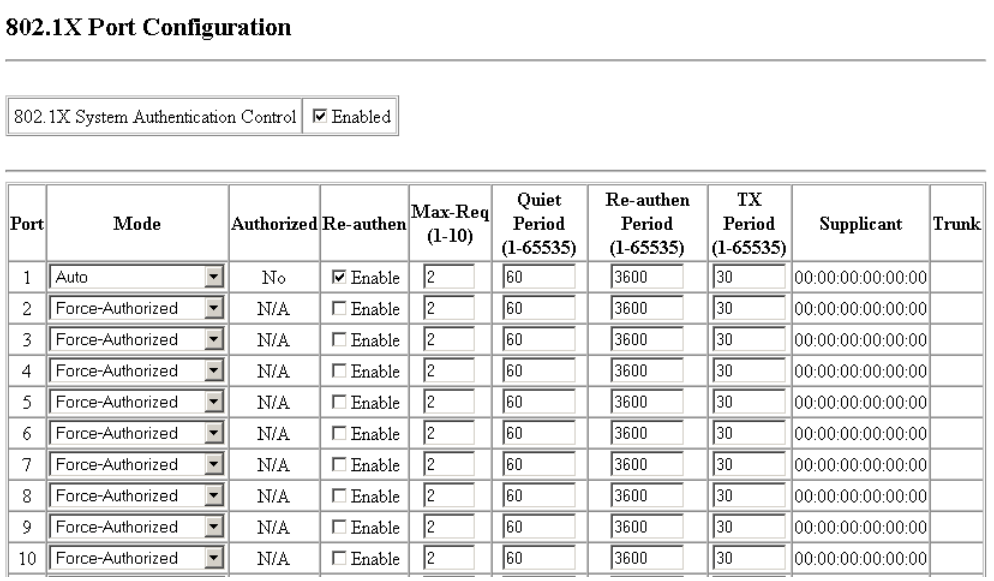
- `Timeout*` - Displays the time interval remaining to the next authentication. (*CLI only)

802.1x Port Configuration via Web

- Open `Security - 802.1x - Port Configuration` - enable/disable the 801.x System Authentication Control use, select the port mode, re-authentication type and timers. Use `Apply` to commit.

* *Note: Use the `Security - 802.1x - Port-Channel Configuration` in order to configure 802.1x with port-channel.*

Figure 8-8. 802.1x Port Configuration via Web



802.1x Port Configuration via CLI

- The next example enables the use of 802.1x globally, configures 802.1x parameters and shows the resulting 802.1x status.

Example 8-7. 802.1x Port Configuration via CLI

```
DmSwitch3000(config)#dot1x system-auth-control
DmSwitch3000(config)#dot1x max-req 2
DmSwitch3000(config)#dot1x port-control auto
DmSwitch3000(config)#dot1x re-authentication
DmSwitch3000(config)#dot1x timeout quiet-period 60
DmSwitch3000(config)#dot1x timeout reauth-period 3600
DmSwitch3000(config)#dot1x timeout tx-period 30
DmSwitch3000(config)#show dot1x
Global 802.1x status: enabled.

  Port   Mode          Authorized  Supplicant          Uptime           Timeout
```

```
  1/1    auto          no          none              n/a             n/a

  1/2    force-auth    n/a         none              n/a             n/a

  1/3    force-auth    n/a         none              n/a             n/a

  1/4    force-auth    n/a         none              n/a             n/a

  1/5    force-auth    n/a         none              n/a             n/a

  1/6    force-auth    n/a         none              n/a             n/a

  1/7    force-auth    n/a         none              n/a             n/a

  1/8    force-auth    n/a         none              n/a             n/a

  1/9    force-auth    n/a         none              n/a             n/a

  1/10   force-auth    n/a         none              n/a             n/a

--More--
DmSwitch3000(config)#
```

8.6. Restricting Management Access

By default, this switch allows access to the management interface to any authenticated user. In order to improve security, it is very interesting to restrict access only to management machines. This task can be accomplished by creating an IP filter entry that allows only some network clients to access the management interfaces. You can create IP filters for any management interface, including Web Configuration, SNMP, Telnet and SSH.

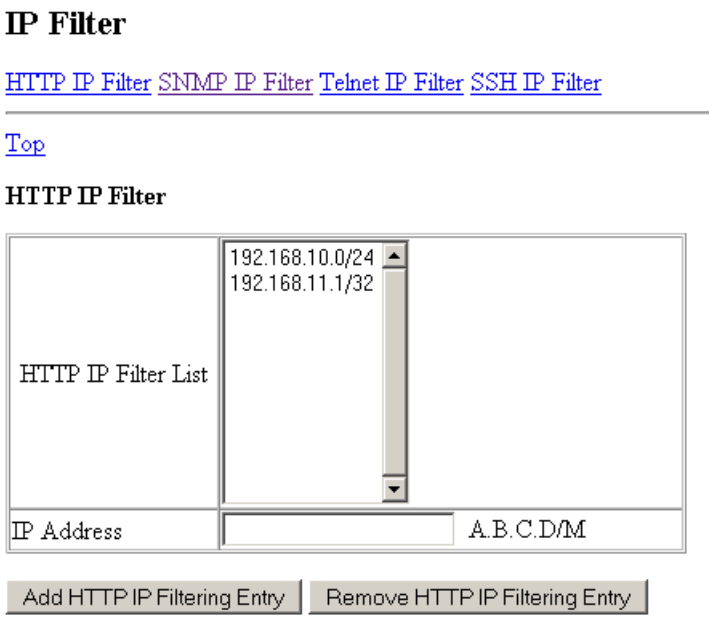
Command Attributes

- `HTTP IP Filter List` - The current list of IPs allowed to access the Web Configuration interface.
- `SNMP IP Filter List` - The current list of IPs allowed to access the SNMP Configuration interface.
- `Telnet IP Filter List` - The current list of IPs allowed to access the Telnet Configuration interface.
- `SSH IP Filter List` - The current list of IPs allowed to access the SSH Configuration interface
- `IP Address` - An IP address in the format A.B.C.D/M, where M is the network mask that establishes a sequence of allowed machines (one or more).

Restricting Management Access via Web

- Open `Security - IP Filter` - Choose a filter box (HTTP, SNMP, Telnet or SSH) and enter a valid IP/Mask. Click on the respective `Add` action. You can also select an already existing entry and click `Remove`.

Figure 8-9. Restricting Management Access via Web



Restricting Management Access via CLI

- The next example creates a new HTTP IP filter entry that grants access to the Web Configuration Interface for the hosts from 192.168.10.1 to 192 .168.10.254. It also creates a specific entry for the host 192.168.11.1

Example 8-8. Restricting Management Access via CLI

```
DmSwitch3000(config)#management http-client 192.168.10.0/24
DmSwitch3000(config)#management http-client 192.168.11.1/32
DmSwitch3000(config)#
```

Chapter 9. SNMP

The Simple Network Management Protocol (SNMP) is a widely used communication protocol built for remote management and monitoring of network equipment (e.g. switches, routers, modems, etc.). A Network Management Station (NMS) running an SNMP application accesses the built-in SNMP agent of the remote managed device by reading from and writing to a called community. The community access string act as a password for the NMS, allowing read-only or read-write access rights. Only network devices that have configured community access strings can be managed/monitored via SNMP. Some SNMP network devices can also be configured to automatically send information (called traps) about special events (e.g. interface status up/down) to the NMS. This switch incorporates an onboard SNMP agent that regularly monitors its hardware and software modules as well as its interfaces, allowing a NMS to manage/monitor it via SNMP. It can also be configured to send SNMP traps to a remote NMS.

9.1. Configuring SNMP Community Access Strings

This switch can be configured with up to five SNMP community access strings. You must set the proper name and access mode for each entry. Remember that community access strings act as passwords for SNMP purposes, so you should replace the default entries by your own.

Command Attributes

- `Community String` - The string to be used by the NMS to manage this switch. Maximum 32 characters, case sensitive.
- `Access Mode`:

  `Read/Write` - NMS is authorized to change and retrieve SNMP MIB objects from the switch.

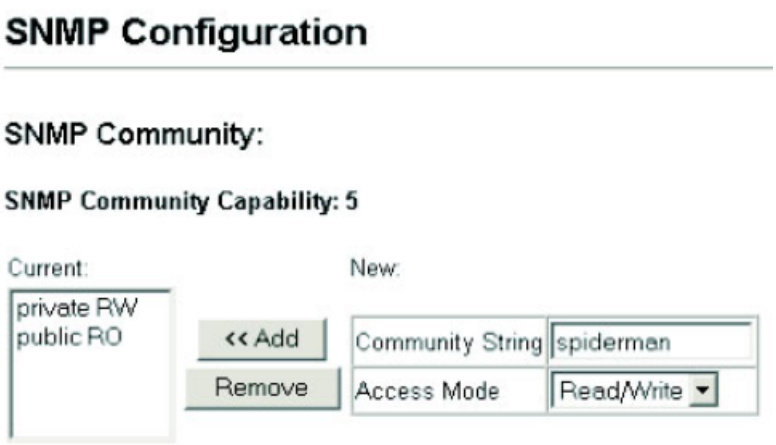
  `Read-Only` - NMS is authorized only to retrieve SNMP MIB objects from the switch.

- `SNMP Community Capability` - Display the maximum number of community strings supported by the switch.

Configuring via Web

- Open `SNMP - Configuration` , fill in the community string name and set the appropriate permission from the `Access Mode` drop-down menu. Click `Add` to commit.

Figure 9-1. Configuring SNMP Community Access Strings via Web



Configuring via CLI

- The next example illustrates how to add the community string "user" with read-only access.

Example 9-1. Configuring SNMP Community Access Strings via CLI:

```
DmSwitch3000(config)#ip snmp-server community user ro
DmSwitch3000(config)#
```

9.2. Setting SNMP Traps

A Trap is a notification sent by a SNMP agent to a NMS indicating that an important event has occurred. In order to implement this functionality, you must set the NMS IP addresses and community names as well as the SNMP trap version format to be sent.

This switch can send several types of traps and up to five NMS can be configured to handle this traps. The traps the switch can send are:

- Power-On
- Link-Up/Link-Down
- Authentication
- Cold and Warm Start
- Configuration change or save
- Fan status change

- Forbidden access
- Login fail and success
- SFP presence
- Stack attach and detach
- Alarm status change
- Traps lost

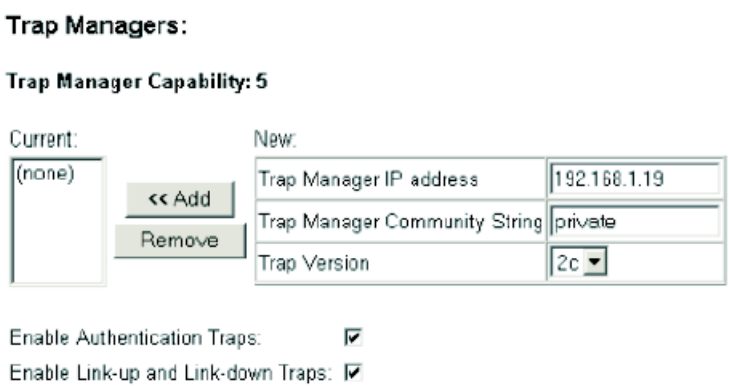
Command Attributes

- `Network Management Station Capability` - Display the maximum number of NMS trap receivers supported by the switch.
- `Trap Receiver IP Address` - The IP address of a NMS that will receive the traps sent by this switch.
- `Trap Receiver Community String` - Traps will be sent to the NMS pertaining to this community string.
- `Trap Version` - Choose whether to send traps as SNMP v1 or 2c.
- `Enable Power-On Traps` - Send a trap when the switch is Powered-On.
- `Enable Link-Up/Link-Down Traps` - Send a trap when a link becomes Up or Down.
- `Enable Authentication Traps` - Send a trap each time a invalid SNMP community string is submitted during the SNMP authentication procedure.
- `Current` - This box displays the already configured trap managers.

Configuring via Web

- Open `SNMP - Configuration` , fill in the `Trap Receiver IP Address` and `Trap Receiver Community String`. Choose the `Trap version` type then click `Add` to commit.

Figure 9-2. Configuring SNMP Trap Receivers



Configuring via CLI

- The following example illustrates how to add a trap receiver and enable traps.

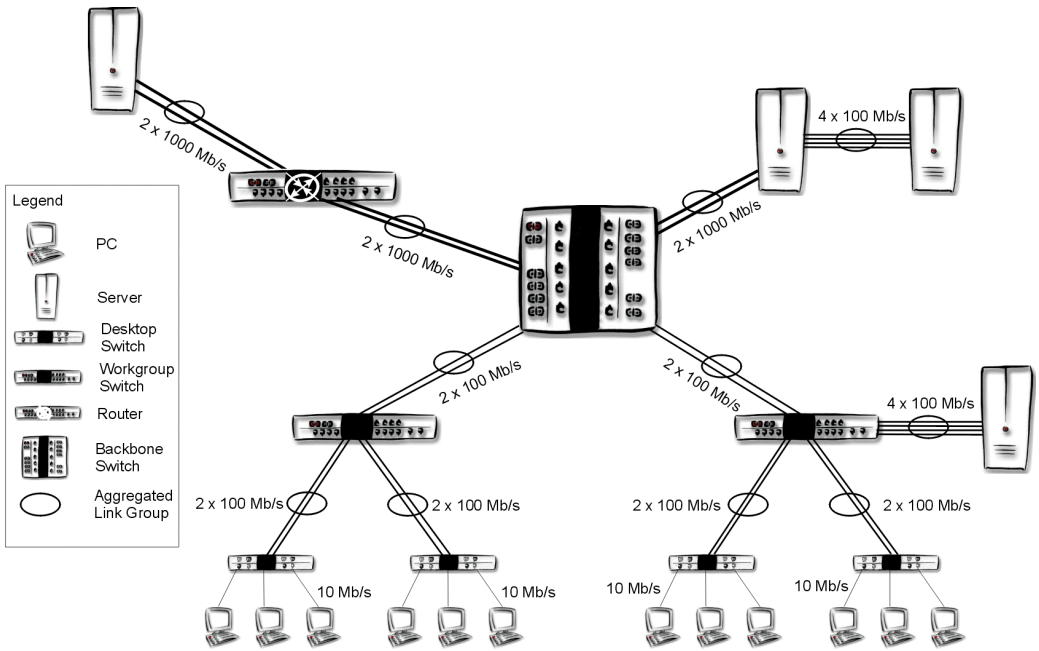
Example 9-2. Configuring SNMP Trap Receivers via CLI:

```
DmSwitch3000(config)#ip snmp-server host 192.168.10.103 private version 2c
DmSwitch3000(config)#ip snmp-server enable link traps
DmSwitch3000(config)#ip snmp-server enable poweron traps
DmSwitch3000(config)#ip snmp-server enable authentication traps
DmSwitch3000(config)#
```

Chapter 10. Link Aggregation

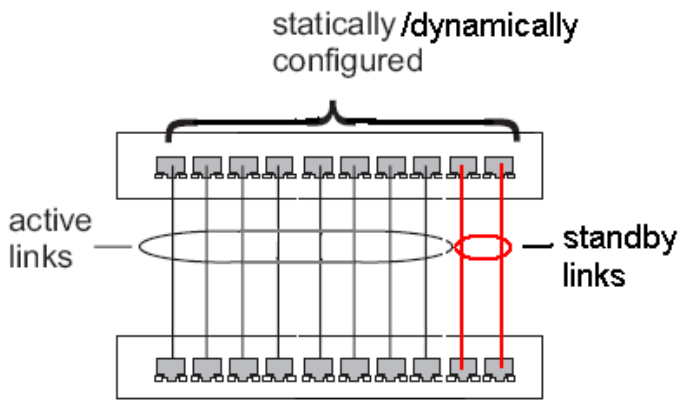
The link aggregation feature allows you to create resilient logical links on the network, improving availability and performance. A link aggregation port acts as a single link for management purposes, though being generally composed of more than one physical link. By combining multiple links into one logical link, Link Aggregation can drastically improve the bandwidth available. It can be used to fix bottlenecks on the network, alleviate traffic exchanged among switches or even improve availability and bandwidth for access servers.

Figure 10-1. Link Aggregation Use Cases



The most common types of link aggregation are static port-channels and dynamic port-channels. Static port-channels have to be manually configured at both ends of the port-channel, and the switch or network interface must comply with the Cisco EtherChannel standard. Dynamic port-channels use *Link Aggregation Control Protocol (LACP)*, defined by IEEE 802.3ad standard. Ports configured with LACP automatically create port-channels with other LACP devices. When more than eight ports constitute a single port-channel (static or dynamic) each new added port will be stated as standby, i.e, will only be used in case one of the 8 ports fail.

Figure 10-2. Port-Channel with Active and Standby Ports



* *Notes:*

* *- You must configure and treat port-channels as point-to-point links. Multipoint Aggregations (aggregations among more than two systems) will not work properly.*

* *- A Port can only be assigned to one port-channel.*

* *- Link Aggregation is supported only on point-to-point links operating in full duplex mode. Use of half duplex operation is not recommended.*

* *- All links in a port-channel must operate at the same data rate (e.g. 10 Mb/s,100 Mb/s, or 1000 Mb/s).*

* *- In order to prevent a network loop creation, first configure the port-channel member ports and then connect the cables. In order to prevent data loss while removing a port from a port-channel, remove the cable first, then remove the port via management software.*

* *- RSTP, VLAN, IGMP, GVRP settings are made for the entire port-channel.*

This switch supports the following Link Aggregation features:

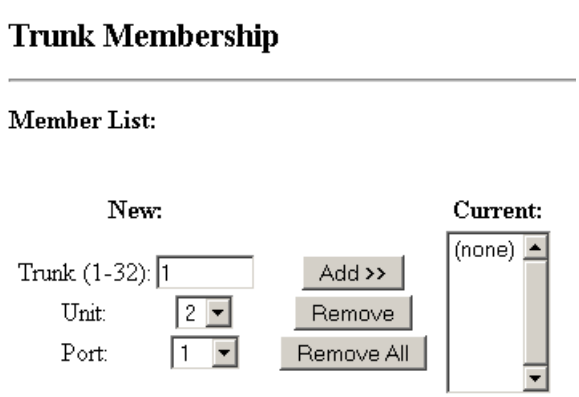
- Cisco EtherChannel for static port-channels
- IEEE 802.3ad LACP - Link Aggregation Control Protocol
- Maximum port-channels per stack: 32
- Maximum forwarding ports per port-channel: 8
- Maximum standby ports per port-channel: unlimited

10.1. Static Port-Channel Configuration

Configuring Static Port-Channel Membership via Web

- Open `Interfaces - Port-Channel Membership` , enter a port-channel and port number to be statically added/removed (or select an existing member from the Current box). Click `Add/Remove/Remove All` to commit.

Figure 10-3. Configuring Static Port-Channel Membership via Web



Configuring Static Port-Channel Membership via CLI

- The next example creates a new port-channel 1, add/removes member ports, and removes port-channel 2 via CLI.

Example 10-1. Configuring Static Port-Channel Membership via CLI

```
DmSwitch3000(config)#interface port-channel 1
DmSwitch3000(config-if-port-ch-1)#set-member ethernet 1/1
DmSwitch3000(config-if-port-ch-1)#set-member ethernet range 1/2 1/3
DmSwitch3000(config-if-port-ch-1)#exit
DmSwitch3000(config)#no interface port-channel 2
DmSwitch3000(config)#exit
DmSwitch3000#show interfaces status port-channel 1
Information of Port-Channel 1
 Basic information:
  Port type:              100TX
  MAC address:            00:04:DF:00:31:01
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10M half, 10M full, 100M half, 100M full
  Flow-control:           Disabled
  MDIX:                   Auto
 Current status:
  Created by:             User
  Link status:            Down
```

```
  Members:                Eth1/1 to Eth1/3

DmSwitch3000#
```

* *Note: A new Port-Channel uses the configuration from the first port that is added to it. The following added ports will use the port-channel active configuration. When removed from the port-channel, ports will use the default configuration.*

10.2. LACP

10.2.1. Configuring LACP

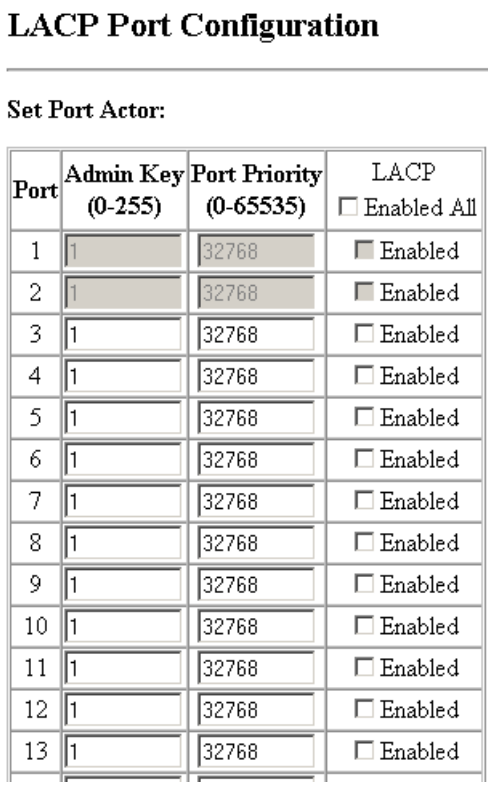
Command Attributes

- `Admin Key` - A unique key shared among ports on the same port-channel. Different port-channels should have different keys.
- `Port Priority` - When more than 8 ports are constituting an aggregate, the lower the value, the more likely that the port will be in the active state.
- `Enabled` - Enable this option so this port will be able to automatically negotiate port-channels with LACP.

LACP Port Configuration via Web

- Open `Layer 2 - LACP - Configuration` , fill in the `Admin Key` (use different keys to negotiate different port-channels), enter a `Port Priority` and click `Enabled` to use LACP on the interface. Click `Apply` to commit.

Figure 10-4. Configuring LACP via Web



LACP Port Configuration

Set Port Actor:

Port	Admin Key (0-255)	Port Priority (0-65535)	LACP ☐ Enabled All
1	1	32768	☐ Enabled
2	1	32768	☐ Enabled
3	1	32768	☐ Enabled
4	1	32768	☐ Enabled
5	1	32768	☐ Enabled
6	1	32768	☐ Enabled
7	1	32768	☐ Enabled
8	1	32768	☐ Enabled
9	1	32768	☐ Enabled
10	1	32768	☐ Enabled
11	1	32768	☐ Enabled
12	1	32768	☐ Enabled
13	1	32768	☐ Enabled

LACP Port Configuration via CLI

- The next example configures administrative key, port priority values and enables LACP on the interface.

Example 10-2. Configuring LACP via CLI

```
DmSwitch3000(config)#interface ethernet 1/1
DmSwitch3000(config-if-eth-1/1)#lacp actor admin-key 255
DmSwitch3000(config-if-eth-1/1)#lacp actor port-priority 1
DmSwitch3000(config-if-eth-1/1)#lacp
DmSwitch3000(config-if-eth-1/1)#
```

10.2.2. Displaying LACP Information

10.2.2.1. Displaying LACP Port Counters

Field Description

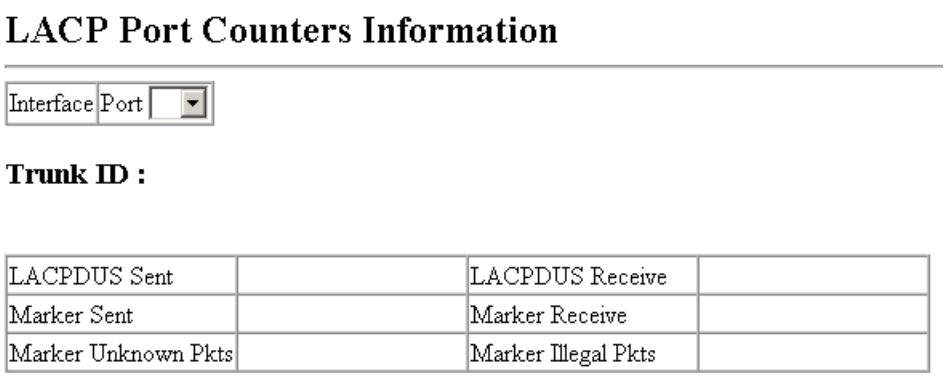
- `LACPDUs Sent` - Number of LACPDUs sent from this port-channel.

- `LACPDUs Received` - Number of LACPDUs received on this port-channel.
- `Marker Response` - Number of Marker PDUs transmitted from this port-channel .
- `Marker Received` - Number of Marker PDUs received by this port-channel .
- `LACPDUs Pkts Err` - Number of LACPDUs received with error.

Displaying LACP Port Counters via Web

- Open `Port - LACP - Port Counters Information`

Figure 10-5. Displaying LACP Port Counters via Web



Displaying LACP Port Counters via CLI

- The next example illustrates how to display LACP Port Counters via CLI.

Example 10-3. Displaying LACP Port Counters via CLI:

```
DmSwitch3000#sh lacp counters
---------------------------------------------------------------------
            LACPDUs         Marker      Marker Response   LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv     Pkts Err
---------------------------------------------------------------------

Aggregator id 1 (channel-group 1)

eth  1/25   156    76       0      0        0      0        0
DmSwitch3000#
```

10.2.2.2. Displaying LACP Port Internal Information

Field Description

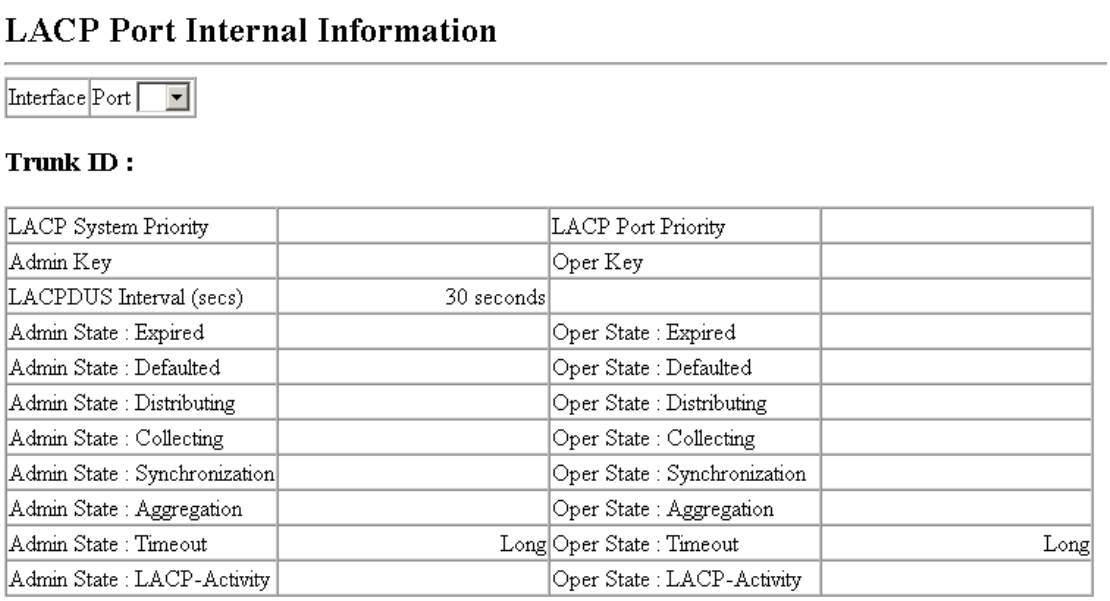
- `Oper Key` - Value of the operational key for the port-channel.

- `Admin Key` - Value of the administrative key for the port-channel.
- `LACP Port Priority` - Value of the LACP port priority within this port-channel.
- `Flags` - Flags indicating the port's mode.
- `Port State` - Set of actor's state parameters.

Displaying LACP Port Internal Information via Web

- Open `Port - LACP - Port Internal Information`

Figure 10-6. Displaying LACP Port Internal Information via Web



LACP Port Internal Information

Interface Port

Trunk ID :

LACP System Priority		LACP Port Priority	
Admin Key		Oper Key	
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted		Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	
Admin State : Collecting		Oper State : Collecting	
Admin State : Synchronization		Oper State : Synchronization	
Admin State : Aggregation		Oper State : Aggregation	
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	

Displaying LACP Port Internal Information via CLI

- The next example illustrates how to display LACP Port Internal Information via CLI.

Example 10-4. Displaying LACP Port Internal Information via CLI:

```
DmSwitch3000#sh lacp internal
Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs
       A - Device is in Active Mode          P - Device is in Passive mode

Port state: A - LACP_Activity   T - LACP_Timeout  G - Aggregation  E - Expired
            S - Synchronization D - Distributing  C - Collecting   F - Defaulted


Aggregator id 1 (channel-group 1)

                    LACP port   Admin     Oper      Port     Port
Port        Flags   Priority    Key       Key       Number   State
```

```
eth  1/25   SA      32768       0x100     0x103     25       AGSCD
DmSwitch3000#
```

10.2.2.3. Displaying LACP Port Neighbors Information

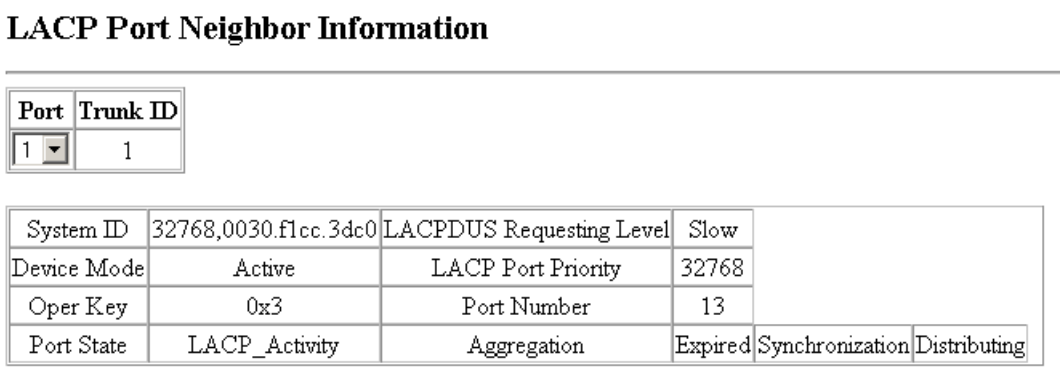
Field Description

- `System ID` - System ID used by the neighbor.
- `Flags` - Flags indicating the neighbor port mode.
- `LACP Port Priority` - LACP port priority assigned to this interface within the channel group.
- `Oper Key` - Value of the neighbor operational key for the port-channel.
- `Port Number` - Port number of the neighbor peer.
- `Port State` - Set of neighbor port state parameters.

Displaying LACP Port Neighbors Information via Web

- Open `Port - LACP - Port Neighbors Information`

Figure 10-7. Displaying LACP Port Neighbors Information via Web



LACP Port Neighbor Information

Port	Trunk ID
1	1

System ID	32768,0030.f1cc.3dc0	LACPDUS Requesting Level	Slow		
Device Mode	Active	LACP Port Priority	32768		
Oper Key	0x3	Port Number	13		
Port State	LACP_Activity	Aggregation	Expired	Synchronization	Distributing

Displaying LACP Port Neighbors Information via CLI

- The next example illustrates how to display LACP Port Neighbors Information via CLI.

Example 10-5. Displaying LACP Port Neighbors Information via CLI:

```
DmSwitch3000#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs
       A - Device is in Active Mode          P - Device is in Passive mode

Port state: A - LACP_Activity   T - LACP_Timeout  G - Aggregation  E - Expired
```

```
            S - Synchronization D - Distributing  C - Collecting   F - Defaulted


Aggregator id 1 (channel-group 1)

Partner's information:

            System                        LACP port   Oper      Port     Port
Port        ID                    Flags   Priority    Key       Number   State
eth  1/1    32768,0030.f1cc.3dc0  SA      32768       0x3       13       AGSCD
DmSwitch3000#
```

Chapter 11. VLAN

Virtual Local Area Networks (VLANs) are logical groups of network nodes implementing separate Layer 2 broadcast domains. Each VLAN is considered a unique broadcast domain, i.e., each network node will only be able to communicate with other nodes that are contained inside the VLAN. A Layer 3 device (e.g, a router) will be necessary in order to establish a connection between different VLANs. In large networks, VLANs help to contain broadcast traffic, optimizing the network resources usage. By Isolating network groups into VLANs you can also improve network security.

This switch supports the following VLAN features:

- Automatic VLAN learning using 802.1Q GARP VLAN Registration Protocol - GVRP
- Maximum of 4094 VLANs
- Port Overlapping
- Multiple VLAN membership
- Bridging between VLAN aware and VLAN unaware equipment
- Port-and-Protocol based VLAN
- MAC-Based VLAN
- Q-in-Q

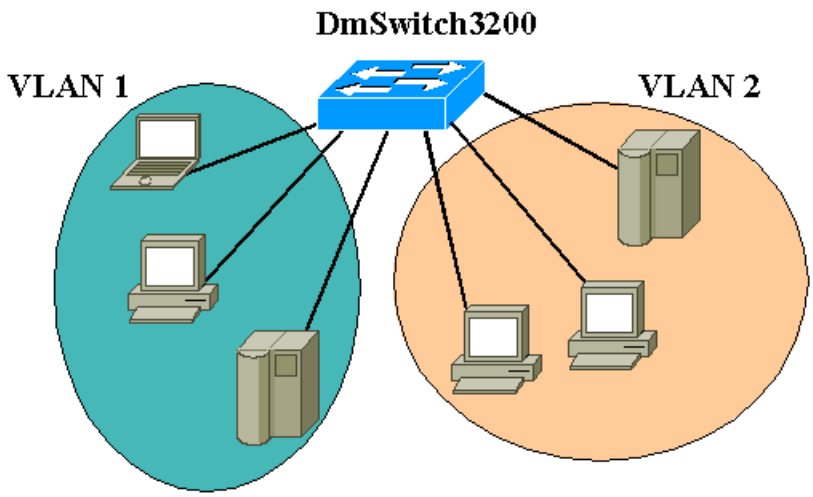
11.1. IEEE 802.1Q VLANs

The IEEE 802.1Q *Virtual Bridged Local Area Networks* standard proposes a way for marking MAC layer frames allowing a switch to propagate VLAN information among other vendor-specific compliant switches. A 802.1Q VLAN works adding a mark called *Tag* to ethernet frames across switches. This tag carries an identifier called *VLAN Identifier - VID* that contains information about the VLAN membership of the frame, allowing switches to forward frames only to ports that are members of the specified VID. When the switch receives a frame it checks the presence of the 802.1Q tag on it. If present (*tagged*), the frame is forwarded directly to the remaining member ports of the VLAN ID. If absent (*untagged*), the frame is forwarded to all remaining member ports from the default VID of the receiving port.

A *Tagged Trunk* is a port that is usually connected to another switch and multiplexes two or more VLAN frames across the network. In order to create a tagged trunk, you must add a port as a tagged member of the VLANs that you want traffic passing through.

A *Port-Based* non-overlapping VLAN is the most simple way to implement VLANs. For each switch port is assigned one Port VLAN ID that identifies the port group membership. For example, you can create VLANs Marketing and Engineering (IDs 2 and 3 respectively), so people from Marketing department will not be able to communicate via Layer 2 with people from Engineering department. Then you can assign the ports 1-10 for Marketing VLAN and 11-20 to Engineering VLAN. The main advantages using this method are the easy start-up configuration and centralized administration. However, with the growing number of VLANs and port utilization/reassignment, this technique becomes harder to manage.

Figure 11-1. A Port-Based non-overlapping VLAN



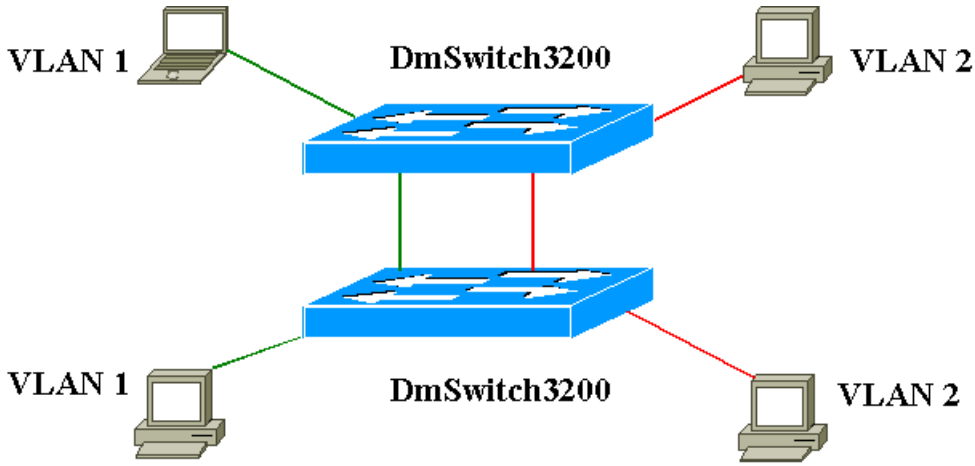
Example 11-1. Port-Based non-overlapping Design

The next table exemplifies a network design based on Port-Based non-overlapping VLAN. In this scenario, both Marketing and Engineering personnel will have granted access to is own servers and printers but will not be able to communicate to each other.

Port	1-10 (Engineering)	11-20 (Marketing)
VID	2	3
VLAN 2 Table	Untagged	Not Member
VLAN 3 Table	Not Member	Untagged

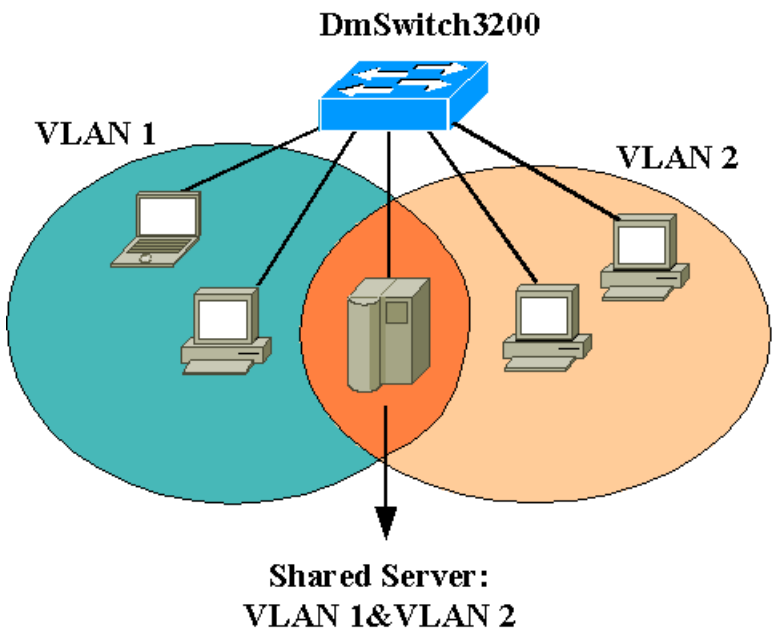
Port-based non-overlapping VLANs also have problems extending along other switches, because requires using an exclusive port for each VLAN connection to another switch. This scenario can become a problem when using the Spanning-Tree Algorithm, because it will probably block all redundant paths between switches.

Figure 11-2. Extending a Port-Based non-overlapping VLAN



The use of 802.1Q VLANs allows the *Port-Overlapping* use. This mean that ports can belong to more than one VLAN, allowing, for example, printers or servers to be shared among separate VLANs. The only requirement is that the device's network card using port-overlapping must be 802.1Q compliant.

Figure 11-3. Using 802.1Q VLAN Port-Overlapping



Example 11-2. Port-Overlapping VLAN Design

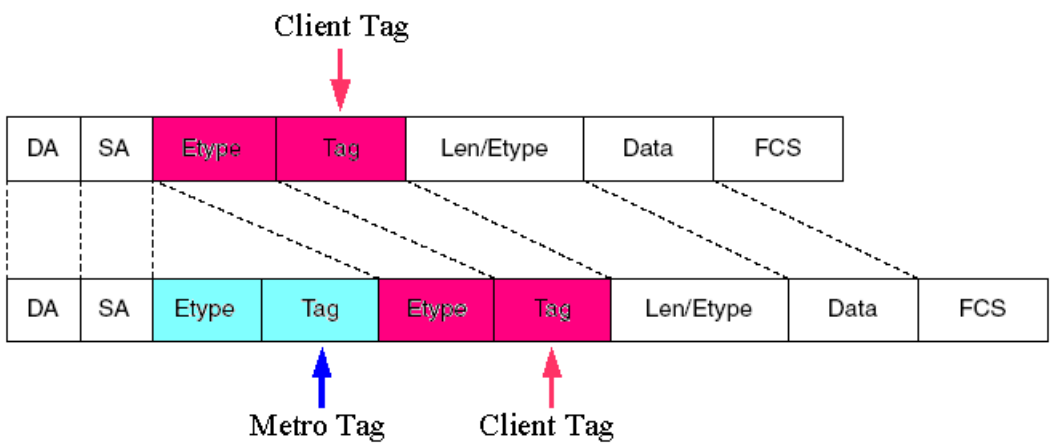
The next table exemplifies a network design based on Port-Overlapping VLAN feature. In this scenario, both Marketing and Engineering personnel will have granted access to the shared printer and server but will not be able to communicate to each other. Note that the shared resources (server, printer, etc..) must have 802.1Q network interface cards (VLAN-aware devices).

Port	1-10 (Engineering)	11-20 (Marketing)	21-22 (Server, Printer)
VID	2	3	Do not care
VLAN 2 Table	Untagged	Not Member	Tagged
VLAN 3 Table	Not Member	Untagged	Tagged

11.1.1. Q-in-Q

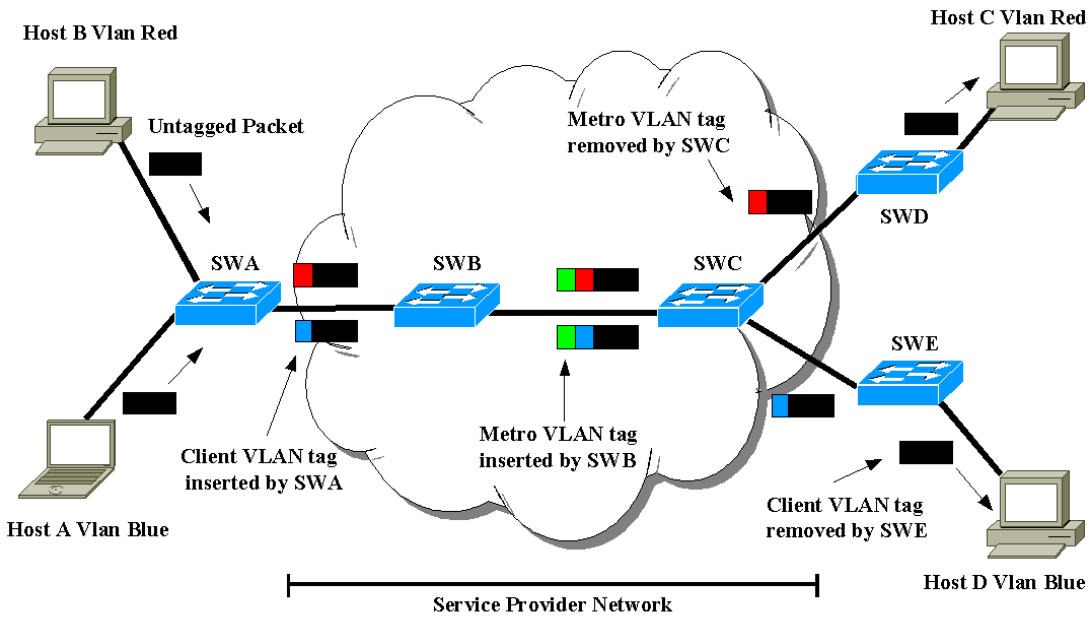
Usually, the service provider costumer has specific VLANs on its network and want to communicate with its other remote VLANs through the provider network . One way to resolve this problem is to directly forward the costumer tagged traffic into the provider network. This solution brings one problem: with the growing demand of VLANs by the clients, the 4094 VLANs address space would be quicly exausted. Another way to resolve this issue is by using the Q-in-Q feature.

Figure 11-4. Q-in-Q frame tagging



Q-in-Q is an encapsulation method that allows a service provider to offer transparent tunneling of client VLANs data through its core network. This is done by adding a second outer VLAN tag, also called Metro Tag. All client VLAN-tagged frames are marked with its specific Metro Tag (assigned transparently by the service provider) and then switched through the provider network until reach its destination (the remote client interconnection point), where the Metro Tag is extracted and the original tagged frame is forwarded.

Figure 11-5. Q-in-Q framework



11.1.2. When to Create 802.1Q VLANs

Use 802.1Q tagged VLANs only when connecting VLAN aware devices (e.g 802.1Q compliant switches/network cards). Setting a port as tagged for a specific VLAN means that the switch will always forward a tagged frame out this port when receiving a frame for this VLAN in another member port. Access ports connected to hosts that are VLAN unaware must be set to untagged.

11.1.3. Rules for Creating 802.1Q VLANs

When creating 802.1Q VLANs keep in mind that:

- Each VLAN has its own unique VID;
- One port can belong to any tagged or untagged 802.1Q VLAN;

- One port must belong to at least one VLAN (either tagged or untagged);
- When the interface `Acceptable Frame Type` parameter is set to tagged, the PVID value is ignored.

11.1.4. Three Basic Steps to Configure 802.1Q VLANs

Follow this three basic steps to successfully configure VLANs

- Create one VLAN ID for each VLAN you need;
- Add ports to created VLANs: each port must be configured as tagged, untagged, forbidden or not member, respecting the mentioned rules;
- Configure each port separately: assign a PVID and the acceptable frame format to be received by the port.

11.2. Displaying VLAN Information

11.2.1. Displaying Current VLAN Configuration

Use the VLAN Configuration page to see separate information for each VLAN on the switch.

Field Description

- `VLAN ID` - Displays all the currently configured VLAN IDs (static or dynamic learnt).
- `IP Address` - Displays the IP Address currently configured (optional).
- `Type` - Displays how the VLAN was added to the switch:

  `Dynamic`: Automatically learnt by GVRP.

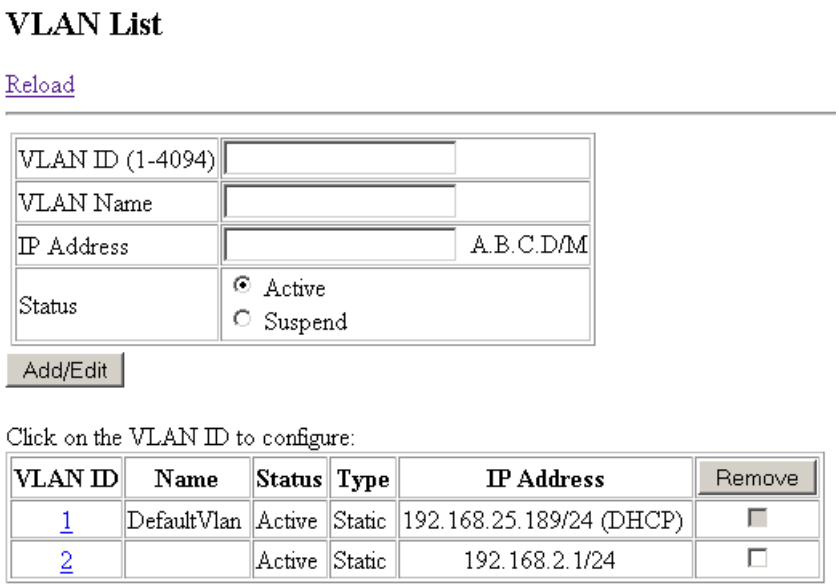
  `Static`: Statically configured by an administrator.

- `Egress Ports` - The current set, type and tagging type of member ports.

Displaying via Web

- Open `VLAN - VLAN List`

Figure 11-6. Displaying VLAN Configuration via Web



Displaying via CLI

- The next example illustrates how to display Current VLAN Information via CLI.

Example 11-3. Displaying Current VLAN Information via CLI:

```
DmSwitch3000#show vlan id 1
VLAN ID:            1
Type:               Static
Name:               DefaultVlan
Status:             Active
IP Address:         192.168.25.189/24
Members:            Eth1/2 to Eth1/28 (static, untagged)
DmSwitch3000#
```

11.3. VLAN Creation

The VLAN Configuration page allows you to create a VLAN by specifying a valid VID. You can also configure a VLAN name up to 32 characters. You must set the VLAN status to `Active` if you want it to forward frames. You can edit a VLAN status by selecting the desired VLAN and changing its status box. You can also create an IP address for accessing the management interface from this VLAN.

Command Attributes

- `VLAN ID` - Choose a valid VLAN ID (range: from 2 to 4094).
- `IP Address` - Fill in a valid IP address and Subnet Mask (optional) This address will be used in order to access the management interface from this VLAN.
- `State` - Select whether to Activate or Suspend the frame forwarding for this VLAN.
- `Remove` - Destroy the selected VLAN. All ports which are using this PVID will be transferred to the DefaultVlan PVID 1.

* *Notes:*

* *- Only the PVID of the ports which were using the destroyed VLAN ID will be changed to PVID 1. Ports which were exclusively egress members (either tagged or untagged) of the destroyed VLAN will be also automatically set to untagged member of VLAN 1.*

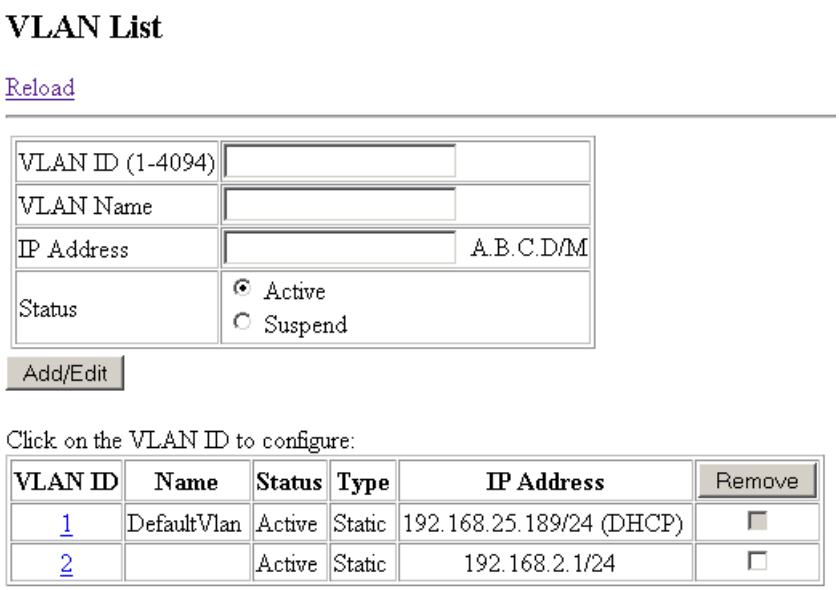
* *- The VLAN 1 (DefaultVlan), Dynamic VLANs entries and Static VLANs with dynamic member ports can not be removed or disabled.*

* *- By changing a Dynamic VLAN entry, it will be automatically changed to a static type.*

Configuring via Web

- Open `VLAN - VLAN Configuration` , fill in the `Vlan ID`, `VLAN Name` and desired `Status`. Optionally you can set an `IP Address` for management purposes or select one VLAN from the `Current List` to edit. Click `Add/Edit` to commit. You can also remove a VLAN by selecting it and pressing the `Remove` button.

Figure 11-7. Creating a VLAN via Web



Configuring via CLI

- The next example illustrates how to create a VLAN with ID 2 named "engineering" and add a IP address via CLI.

Example 11-4. Creating a VLAN via CLI:

```
DmSwitch3000(config)#interface vlan 2
DmSwitch3000(config-if-vlan-1)#name engineering
DmSwitch3000(config-if-vlan-1)#ip address 192.168.10.12/24
DmSwitch3000(config-if-vlan-1)#exit
DmSwitch3000(config)#
```

11.4. Adding VLAN Static Member Ports

The Static Table Page allows you to add/remove/change the static VLAN port membership. Add ports as tagged if there are only VLAN-aware devices connected to this VLAN. If there are VLAN-unaware devices connected choose the untagged option. Configure a VLAN as Forbidden to avoid the port to learn this VLAN by GVRP.

Command Attributes

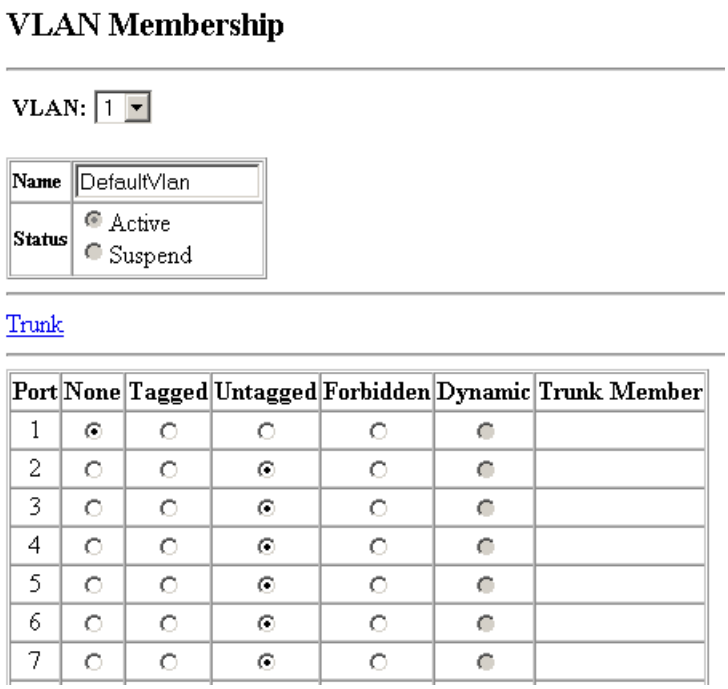
- `VLAN ID` - ID of the VLAN. (1-4094)
- `VLAN Name` (optional) - Display the VLAN name for administrative-only purposes. (1-32 characters)
- `Status` - Select `Active` to begin forwarding of frames or `Suspended` to stop forwarding for the specific VLAN
- `Port` - Port Number
- `Membership` - Select the appropriate VLAN membership for each port or port-channel. Note that you can not change separately ports grouped into port-channels. You can configure port-channels by using the last table on this page.

* *Note: Although you are not allowed to remove a dynamic member port, you can change it to a static type.*

Configuring via Web

- Open `VLAN - VLAN Membership` , select the `Vlan ID`. The correct VLAN name, status and the membership port table will be automatically loaded into the browser. Choose the membership for each port or port-channel and then click `Apply` to commit.

Figure 11-8. Configuring VLAN membership via Web



Configuring via CLI

- The next example illustrates how change the VLAN membership type for interfaces via CLI.

Example 11-5. Configuring VLAN membership via CLI:

```
DmSwitch3000(config)#interface vlan 2
DmSwitch3000(config-if-vlan-2)#set-member tagged ethernet  1/1
DmSwitch3000(config-if-vlan-2)#set-member untagged ethernet  1/3
DmSwitch3000(config-if-vlan-2)interface vlan 3
DmSwitch3000(config-if-vlan-3)#set-member forbidden ethernet  1/3
DmSwitch3000(config-if-vlan-3)#no set-member ethernet  1/1 1/2
DmSwitch3000(config-if-vlan-3)#exit
DmSwitch3000(config)#
```

11.5. VLAN Interface Configuration

The VLAN Interface Configuration Page allows you to configure VLAN-related properties for switch ports. Port-Channel member ports are configured on the VLAN Port-Channel Configuration page.

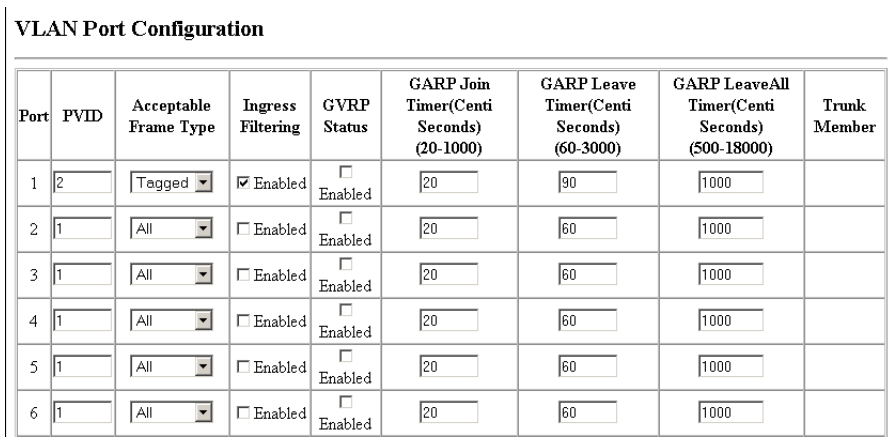
Command Attributes

- `PVID` - The Port VLAN ID must be set to a already created VID and is assigned only to untagged frames received on this port. . If the port is configured to accept tagged frames only, there is no sense to configure this parameter, so any change to it will be ignored.
- `Acceptable Frame Type` - The frame type the port will accept to receive. Choose `All` to accept both tagged and untagged frames. Selecting Tagged will force the switch to discard received untagged frames.
- `Ingress Filtering` - Enable this option to make the switch discard incoming tagged frames from VLANs that the port is not member. Disable this option to make the switch flood non-member incoming frames (note that frames from forbidden VLANs will always be discarded).
- `GVRP Status` - Enables the GVRP for the port. GVRP must also be enabled globally in order to work properly.
- `GARP Join Timer` - The time interval between sending *Join In* messages.
- `GARP Leave Timer` - The time interval a interface waits to leave a joined VLAN.
- `GARP Leave All Timer` - The time interval between sending a *Leave All* message and leaving the VLAN group.
- `Port-Channel Member` - Displays the port aggregation membership. Note that port-channel member ports are configured on the VLAN Port-Channel Configuration page.

Configuring via Web

- Open `VLAN - VLAN Port/Port-Channel Configuration` , fill in the interface configuration then click `Apply` to commit.

Figure 11-9. VLAN Interface Configuration Page



Configuring via CLI

- The next example illustrates how to configure VLAN characteristics for a interface via CLI.

Example 11-6. Configuring VLAN Interface via CLI:

```
DmSwitch3000(config)#interface ethernet 1/1
DmSwitch3000(config-if)#switchport native vlan 2
DmSwitch3000(config-if)#switchport acceptable-frame-type tagged
DmSwitch3000(config-if)#switchport ingress-filtering
DmSwitch3000(config-if)#garp timer join 20
DmSwitch3000(config-if)#garp timer leave 90
DmSwitch3000(config-if)#garp timer leaveall 2000
DmSwitch3000(config-if)#switchport gvrp
DmSwitch3000(config-if)#
```

11.6. GVRP

The *GARP VLAN Registration Protocol* - GVRP - provides 802.1Q automatic VLAN creation and registration on 802.1Q ports. GVRP is defined in the IEEE 802.1P standard and defines a way for switches to learn and propagate VLAN configuration with other GVRP-aware devices, dynamically controlling and creating VLANs on switches across the network.

GVRP works by exchanging messages through 802.1Q trunks. This messages contain information about VLAN membership of the switches. GVRP-aware *Network Interface Cards* (NICs) on hosts also allows automatic VLAN registration/deregistration on GVRP enabled edge switch ports. If it is your case, all you need is to configure the VLAN membership on end stations and enable GVRP on the switch and respective switch ports. If there are no GVRP-aware NICs on hosts, an administrator must statically configure VLANs and GVRP on edge switches and configure only GVRP on intermediate switches.

11.6.1. Enabling GVRP Global Status

In order to enable GVRP, you must first activate it globally on the switch and then activate locally on each interface.

Configuring via Web

- Open `VLAN - GVRP Status` , select the desired status from `GVRP Enable` box. Click `Apply` to commit.

Figure 11-10. Enabling GVRP Global Status via Web

Configuring via CLI

- The next example illustrates how to enable GVRP globally from the CLI.

Example 11-7. Enabling GVRP Global Status via CLI:

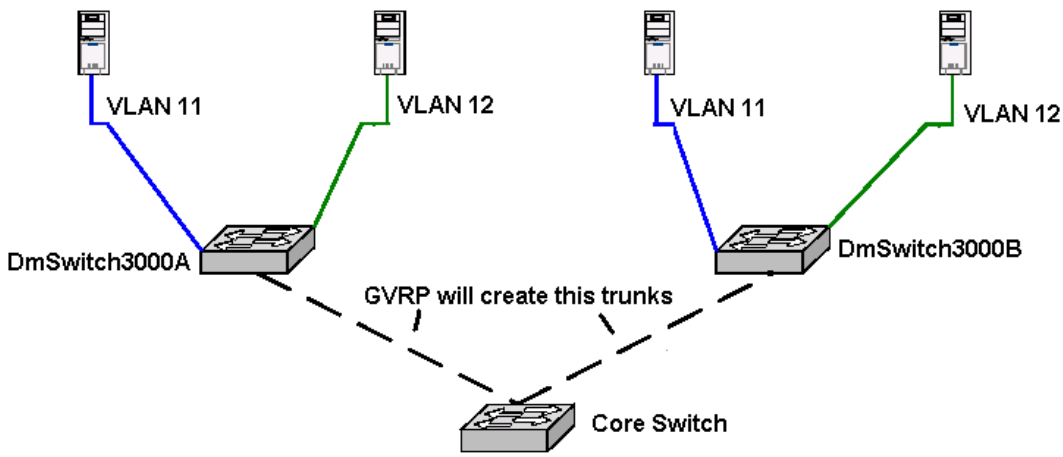
```
DmSwitch3000(config)#bridge-ext gvrp
DmSwitch3000(config)#
```

11.6.2. A GVRP Network Configuration Example

Configuring via CLI

- The following example illustrates how to configure the next GVRP network:

Figure 11-11. A GVRP Network Scenario



Example 11-8. Configuring GVRP from CLI

1. Create the VLANs 11 and 12

On DmSwitch3000A and DmSwitch3000B:

```
DmSwitch3000(config)#interface vlan 11
```

```
DmSwitch3000(config-if-vlan-11)#name engineering
DmSwitch3000(config-if-vlan-11)#interface vlan 12
DmSwitch3000(config-if-vlan-12)#name marketing
DmSwitch3000(config-if-vlan-12)#exit
DmSwitch3000(config)#
```

2. Add Static Member Ports to VLANs:

   On DmSwitch3000A and DmSwitch3000B:

```
DmSwitch3000(config)#interface vlan 11
DmSwitch3000(config-if-vlan-11)#set-member untagged ethernet 1/2
DmSwitch3000(config-if-vlan-11)#interface ethernet 1/2
DmSwitch3000(config-if-eth-1/2)#switchport native vlan 11
DmSwitch3000(config-if-eth-1/2)#interface vlan 12
DmSwitch3000(config-if-vlan-12)#set-member untagged ethernet 1/3
DmSwitch3000(config-if-vlan-12)#interface ethernet 1/3
DmSwitch3000(config-if-eth-1/3)#switchport native vlan 12
DmSwitch3000(config-if-eth-1/3)#exit
DmSwitch3000(config)#
```

3. Enable GVRP globally and on each interface:

   On DmSwitch3000A and DmSwitch3000B:

```
DmSwitch3000(config)#bridge-ext gvrp
DmSwitch3000(config)#interface ethernet 1/1
DmSwitch3000(config-if-eth-1/1)#switchport gvrp
DmSwitch3000(config-if-eth-1/1)#interface ethernet 1/2
DmSwitch3000(config-if-eth-1/2)#switchport gvrp
DmSwitch3000(config-if-eth-1/2)#interface ethernet 1/3
DmSwitch3000(config-if-eth-1/3)#switchport gvrp
DmSwitch3000(config-if-eth-1/3)#exit
DmSwitch3000(config)#
```

4. Enable VLAN trunking (tagging) on intermediate switch/interfaces.
5. Enable GVRP on intermediate switches/interfaces.

Chapter 12. Spanning Tree

In a bridged network the use of a *Spanning Tree Algorithm (STA*) is usually vital to improve network dependability and resiliency. The main purpose of this algorithm is to avoid the creation of network loops while guaranteeing end-user availability. In fact, active network loops in a bridged network are highly undesired because they bring problems like *Broadcast Storms* and *Duplicate Unicast Frame Transmissions*. However, network managers usually need to implement redundant links in order to improve dependability. By allowing the assignment of network backup links, a STA can also improve network resiliency. Being implemented on the Layer 2, the first standard for a *Spanning Tree Protocol (STP)* was released by the IEEE committee 802.1D. The next standard, *Rapid Spanning Tree Protocol (RSTP)* was released under the 802.1W IEEE specification and it is a major improve to the old and slow STP. You should consider using the RSTP protocol implementation whenever possible.

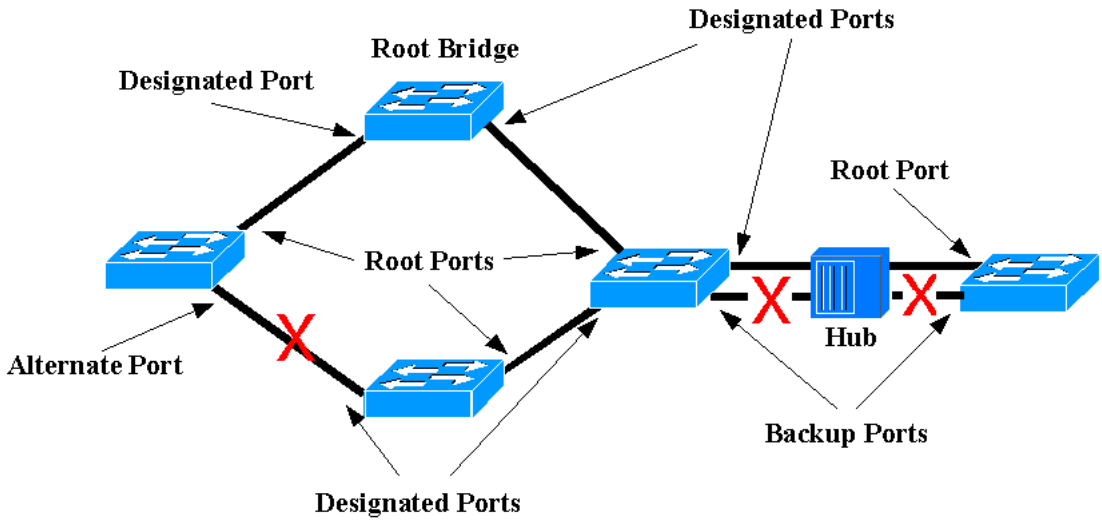
This switch supports the following STA features:

- IEEE 802.1D STP - Spanning Tree Protocol (per VLAN)
- IEEE 802.1w RSTP - Rapid Spanning tree Protocol (per VLAN)
- IEEE 802.1s MSTP - Multiple Spanning Tree Protocol

12.1. How STP Works

STP is a distributed algorithm that create a loop-free bridged network. It achieves this by creating a spanning tree structure on the network. Initially, by exchanging *Bridge Protocol Data Units - BPDUs*, a single *root bridge* is selected among all connected participating bridges. Based on this information, each remaining bridge selects a *root port*, i.e., a port with the lowest cost that leads to the root bridge. Next, each bridge determines which ports will be designated for their corresponding LANs. Both root and designated ports will be put in the *forwarding state*. All remaining ports will be put in the *blocked state*. By blocking all redundant paths STP guarantees a loop-free topology.

Figure 12-1. Maintaining a Loop-Free Topology by Using STP



12.2. Differences Between RSTP and STP

RSTP is a improvement to the legacy STP. It is able to reduce the time until convergence and reconfiguration of the topology occurs by implementing alternate and backup type ports, reducing port states, enabling explicit proposal/agreement sequences on new designated ports and enabling instant forwarding on edge ports. The topology change mechanism was also improved, allowing a rapid propagation of topology change information along the network.

RSTP is fully compatible with legacy STP bridges. Whenever a STP bridge is detected by a RSTP bridge, the later will automatically start to send STP compatible BPDUs, guaranteeing a stable and loop-free network.

12.3. Displaying STA Information

The STA Information pages allow you to see the parameters and states related to STA.

12.3.1. Displaying STA Global Properties

The following STA Global Properties can be displayed:

Command Attributes

- `Spanning Tree Mode` - Whether the STA is RSTP (recommended), STP (legacy STP compatibility mode) or MSTP.
- `MST Name` - Dislay the MST region name.
- `MST Revision Version` - The MST region revision number.

Displaying via CLI

- The next example illustrates how to display Spanning Tree Global Information via CLI.

Example 12-1. Displaying Spanning Tree Information via CLI:

```
DmSwitch3000#show spanning-tree

Spanning-tree information
-------------------------
 Spanning tree mode: RSTP
 MST name:           test
 MST revision:       1

DmSwitch3000#
```

12.3.2. Displaying STA Instance Information

Use the STA Instance Information page to see the STA instance parameters configured on the switch.

Field Description

- `Spanning Tree Mode` - Whether the STA instance is RSTP (recommended), STP (legacy STP compatibility mode) or MSTP.
- `Spanning Tree State` - The STA instance State.
- `Bridge ID` - The bridge ID of the instance. (Will be submitted by this switch in the next root bridge election). It is the concatenation of the configured bridge priority and the bridge MAC address.
- `Max Age` - When the Max Age timer expires on a port, this port starts the process to become a Designated Port for its segment. If it is the root port, a new root port election will be executed.
- `Hello Time` - The time interval between two consecutive configuration messages sent by the root bridge.(Or by this bridge, when it becomes the root bridge).
- `Forward Delay` - In a worst case scenario, the STA instance waits the expiration of this timer to transit a port from blocking state to learning state, and from learning state to forwarding state.
- `Designated Root` -The root bridge ID of the spanning tree instance topology. (When STA is not enabled for an instance, this value is equal to the bridge ID of it).
- `Root port` - The bridge port number that leads to the root bridge.
- `Root path Cost` - The path cost to reach the root bridge.
- `Number of Topology Changes` - Number of reconfigurations of the spanning tree instance topology.

- `Last Topology Change` - Time elapsed since the last Topology Change.
- `Members` - The VLAN IDs of the spanning tree instance.

Displaying via CLI

- The next example illustrates how to display Spanning Tree Instance Information via CLI.

Example 12-2. Displaying Spanning Tree Information choosing an Instance via CLI:

```
DmSwitch3000#show spanning-tree 1
Spanning-tree 1 information
----------------------------------------------------------------
 Spanning tree mode:               RSTP
 Spanning tree state:              Enabled
 Priority:                         0
 Bridge Hello Time (sec.):         2
 Bridge Max Age (sec.):            20
 Bridge Forward Delay (sec.):      15
 Root Hello Time (sec.):           2
 Root Max Age (sec.):              20
 Root Forward Delay (sec.):        15
 Designated Root:                  0.0004df0000eb
 Current root port:                0
 Current root cost:                0
 Number of topology changes:       0
 Last topology changes time (sec.) 5201
 Members:                          VLAN 1
----------------------------------------------------------------
```

12.3.3. Displaying STA Instance Port Information

Use the STA Instance Port Information page to see the STA instance port parameters configured.

Field Description

- `STA Admin State` - Displays weather the STA instance is enabled on the port or not.
- `Role` - Shows the port role: Designated (when it transmits traffic to/from this LAN segment through this bridge to the root bridge), Root (a port that is part of the active topology that leads to the root bridge), Alternate or Backup (a port that provides a redundant path on this switch or to another switch in case a active root or designated port fails) and Disabled when the port does not participate in the spanning tree instance.
- `State` - Shows the port state: Blocking (the port does not forward frames), Learning (the port does not forward frames but learns MAC addresses), Forwarding (the port is forwarding frames).
- `Designated Cost` - In order to select the best path possible that leads to the root bridge, the STA uses this parameter to calculate the cost along a port to the root bridge. The port with the lowest designated cost will be selected. This is the cost reported by the designated port on the LAN segment this port is attached to.
- `Priority` - In case the designated cost being equal or greater on more than one port on the switch, the port with the lowest priority value (highest priority) will be selected as member of the active topology.

Whenever more than one port present the same designated cost and priority, the port with lowest number will be selected.

- `Path Cost` - Faster ports should be configured with lower path costs than slower ports.
- `Designated Port` - Priority and number of the designated port on the LAN segment this port is attached to.
- `Designated Root` - Root bridge ID received from the designated bridge of the LAN this port is attached to.
- `Designated Bridge` - Bridge ID of the designated bridge of the LAN segment this port is attached to.
- `Admin Edge Port` - If enabled, the port is considered not to be attached to another bridge, so fast transition to forwarding state will be achieved.
- `Admin Link Type` - Choose `Point-to-Point` if this port is directly attached to another bridge. Choose `Shared` if this port is connected to a shared LAN segment (a segment with three or more bridges, connected by a Hub). Leaving the `Auto` option will result in a point-to-point type link when the port is forced (or auto-negotiates) to full-duplex communication and results in a shared type link when half-duplex mode is operational.
- `Oper Edge Port` - The operational status of the edge (fast forwarding) mode.
- `Oper Link Type` - The operational link type of the port (see the Admin Link Type parameter above for a detailed description of this filed)

Displaying via CLI

- The next example illustrates how to display Spanning Tree Instance Port Information via CLI.

Example 12-3. Displaying Spanning Tree Port Information by selecting an Instance via CLI:

```
DmSwitch3000#show spanning-tree 1 ethernet 1/1
Eth  1/ 1 information
------------------------------------------------------------------
 STA admin state:       Enabled
 Role:                  Disabled
 State:                 Disabled
 Path cost:             200000
 Priority:              128
 Designated cost:       0
 Designated port:       128.1
 Designated Root:       0.000000000000
 Designated Bridge:     0.000000000000
 Admin edge port:       Disabled
 Admin Link type:       auto
 Oper edge port:        Disabled
 Oper Link type:        point-to-point


DmSwitch3000#
```

12.4. Configuring STA

12.4.1. Configuring STA Global Properties

You can configure the following STA Global Properties:

Command Attributes

- `Spanning Tree Type` - Choose whether the instance will use `STP` (802.1D STP), `RSTP` (802.1w RSTP) or MSTP format BPDUs (`RSTP` is the default, `STP` is a compatibility mode).
- `Revision Version` - The MST region revision number.
- `Name` - The MST region name.

Configuring via CLI

- The next example illustrates how to select the spanning tree mode to RSTP, via CLI.

  Example 12-4. Configuring the STA mode

```
DmSwitch3000(config)#spanning-tree mode rstp
DmSwitch3000(config)#
```

- To configure the MST revision to 1 and set its name to "test", the next example illustrates it:

  Example 12-5. Configuring the MST revision and its name

```
DmSwitch3000(config)#spanning-tree mst revision 1
DmSwitch3000(config)#spanning-tree mst name test
```

12.4.2. Configuring STA Instance Properties

Use the STA Instance Configuration page to configure each instance of the STA parameters such as state and timers.

Command Attributes

- `Spanning Tree State` - Enables/Disables the spanning tree instance state.
- `Priority` - Set the desired Bridge Priority of the instance. This value will be used by STA in order to elect the spanning tree root bridge. Lower values represents higher priorities to become the root bridge. If all devices on the network use the same priority, the one with the lowest MAC address will be elected the root bridge.

  - Default: 32768 - Range: 0-61440, in steps of 4096. - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864,40960, 45056, 49152, 53248, 57344, 61440

- `Hello Time` - Set the time interval (in seconds) used by the STA instance (only while being the root bridge) between sending BPDUs.
- `Maximum Age` - Set the Maximum Age parameter (in seconds) for this instance that will be sent on BPDUs by this switch while being the root bridge.
- `Forward Delay` - Set the Forward Delay parameter (in seconds) for this instance that will be sent on BPDUs by this switch while being the root bridge.
- `VLAN Members` - Set the VLAN IDs to add it to a spanning tree instance.

Configuring via CLI

- The next example illustrates how to change the instance 1 of spanning tree bridge priority to 61440 and enable this STA instance via CLI.

* *Note: Timer values are selected by default and can be changed as required.*

Example 12-6. Configuring the Instance 1 of STA Properties

```
DmSwitch3000(config)#spanning-tree 1 priority 61440
DmSwitch3000(config)#spanning-tree 1 hello-time 2
DmSwitch3000(config)#spanning-tree 1 forward-delay 15
DmSwitch3000(config)#spanning-tree 1 max-age 20
DmSwitch3000(config)#spanning-tree 1
DmSwitch3000(config)#
```

- To add VLAN 1 to spanning tree instance 1, the next example illustrates it:

Example 12-7. Adding VLAN 1 to Spanning Tree Instance 1

```
DmSwitch3000(config)#spanning-tree 1 vlan 1
DmSwitch3000(config)#
```

12.4.3. Configuring STA Instance Port Properties

The STA Instance Port Configuration allows you to set specific STA Port parameters for an instance.

Command Attributes

- `Spanning Tree` - Enables/Disables the STA on this port for an specific instance. Default: Enabled
- `Priority` - Set the priority of the port in steps of 16. Default: 128
- `Path Cost` - Set the path cost. Recommended values are: For 10 Mb/s links - Path Cost 2.000.000 For 100 Mb/s links - Path Cost 200.000 For 1 Gb/s links - Path Cost 20.000 For 10 Gb/s links - Path Cost 2.000

- `Admin Link Type` - Choose `Point-to-Point` when the port is connected to only one bridge partner. Choose `Shared` when the port is connected to more than one bridge partner (e.g a port connected to a Hub with 3 bridges). Choose `Auto` to let the switch choose the Admin Link Type based on the link duplex state from the port. Default: `Auto`
- `Admin Edge Port (Fast Forwarding)` - Enable this option whenever the port is attached to a end-station (not a bridge). Default: Disabled

Configuring via CLI

- The next example illustrates how to set, for a spanning tree instance, path cost, link type, port priority and STA administrative state on a interface via CLI.

Example 12-8. Configuring a Port, by choosing the Instance 1 of STA

```
DmSwitch3000(config)#interface ethernet 1/1
DmSwitch3000(config-if-eth-1/1)#spanning-tree 1 cost 200000
DmSwitch3000(config-if-eth-1/1)#spanning-tree 1 link-type point-to-point
DmSwitch3000(config-if-eth-1/1)#spanning-tree 1 port-priority 128
DmSwitch3000(config-if-eth-1/1)#spanning-tree 1
DmSwitch3000(config-if-eth-1/1)#no spanning-tree 1 edge-port
DmSwitch3000(config-if-eth-1/1)#exit
DmSwitch3000(config)#
```

Chapter 13. Ethernet Automatic Protection Switching Configuration

The EAPS protocol provides fast protection switching to layer 2 switches interconnected in an Ethernet ring topology, such as a metropolitan area network (MAN) or large campuses. EAPS protection switching is similar to what can be achieved with the Spanning Tree Protocol (STP), but offers the advantage of converging in less than a second when a link in the ring breaks.

To take advantage of the Spatial Reuse technology and broaden the use of the ring's bandwidth, EAPS supports multiple EAPS domains running on the ring at the same time.

EAPS operates by declaring an EAPS domain on a single ring. Any VLAN that warrants fault protection is configured on all ring ports in the ring, and is then assigned to an EAPS domain. On that ring domain, one switch, or node, is designated the *master* node, while all other nodes are designated as *transit* nodes.

One port of the master node is designated the master node's *primary* port (P) to the ring; another port is designated as the master node's *secondary* port (S) to the ring. In normal operation, the master node blocks the secondary port for all non-control traffic belonging to this EAPS domain. If the master node detects a break in the ring, it unblocks its secondary port and allows data traffic to be transmitted and received through it.

EAPS fault detection on a ring is based on a single *control* VLAN per EAPS domain. This EAPS domain provides protection to one or more data-carrying VLANs called *protected* VLANs. The control VLAN is used only to send and receive EAPS messages; the protected VLANs carry the actual data traffic.As long as the ring is complete, the EAPS master node blocks the protected VLANs from accessing its secondary port.

A master node detects a ring fault in either of two ways:

- Failed response to a periodic health-check packet on the control VLAN
- "Link down" trap message send by a transit node on the control VLAN

When the master node detects a failure, it declares a "failed" state and opens its logically blocked secondary port on all the protected VLANs. The master node also flushes its forwarding database (FDB) and sends a message on the control VLAN to all of its associated transit nodes to flush their forwarding databases.

13.1. Enabling EAPS Globally

Enabling EAPS Globally via Web

- Open `LAYER 2 - EAPS - EAPS Global Configuration`. Mark `EAPS globally enabled for the switch`. Click `Apply`.

Figure 13-1. Enabling an EAPS Globally via Web

Enabling EAPS Globally via CLI

- The next example illustrates how to enable an EAPS globally via CLI.

Example 13-1. Enabling EAPS Globally via CLI

```
DmSwitch3000(config)#eaps
DmSwitch3000(config)#
```

13.2. Disabling EAPS Globally

Disabling EAPS Globally via Web

- Open `LAYER 2 - EAPS - EAPS Global Configuration`. Unmark `EAPS globally enabled for the switch`. Click `Apply`.

Disabling EAPS Globally via CLI

- The next example illustrates how to disable an EAPS globally via CLI.

Example 13-2. Disabling EAPS Globally via CLI

```
DmSwitch3000(config)#no eaps
DmSwitch3000(config)#
```

13.3. Creating an EAPS Domain

The `name` parameter is a character string of up to 32 characters that identifies the EAPS domain to be created. EAPS domain names and VLAN names must be unique. Do not use the same name string to identify both an EAPS domain and a VLAN.

Creating an EAPS via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Mark `Create a new domain` and put the name of the new domain in the text box. Click `Apply`.

Creating an EAPS via CLI

- The next example illustrates how to create an EAPS via CLI.

Example 13-3. Creating an EAPS via CLI

```
DmSwitch3000(config)#eaps datacom
DmSwitch3000(config)#
```

13.4. Deleting an EAPS Domain

Using the following command you will be able to delete EAPS.

Deleting an EAPS via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain to remove, mark `Remove this domain` and click `Apply`.

Deleting an EAPS via CLI

- The next example illustrates how to delete an EAPS via CLI.

Example 13-4. Deleting an EAPS via CLI

```
DmSwitch3000(config)#no eaps datacom
DmSwitch3000(config)#
```

13.5. Enabling EAPS for Domain

Using the following command you will be able to enable EAPS. EDP must be enabled on the switch and EAPS ring ports.

Enabling EAPS for Domain via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to enable, mark `Enabled` for `Domain Operation`. Click `Apply`.

Enabling EAPS for Domain via CLI

- The next example illustrates how to enable EAPS for domain via CLI.

Example 13-5. Enabling EAPS for Domain via CLI

```
DmSwitch3000(config)#eaps datacom enable
DmSwitch3000(config)#
```

13.6. Disabling EAPS for Domain

Using the following command you will be able to disable EAPS for domain. Select the domain you want to disable, unmark `Enabled` for `Domain Operation`. Click `Apply`.

Disabling EAPS for Domain via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to disable, unmark `Enabled` for `Domain Operation`. Click `Apply`.

Disabling EAPS for Domain via CLI

- The next example illustrates how to disable EAPS for Domain via CLI.

Example 13-6. Disabling EAPS for Domain via CLI

```
DmSwitch3000(config)#eaps datacom disable
DmSwitch3000(config)#
```

13.7. Adding a Control VLAN

You must configure one *control* VLAN for each EAPS domain. The control VLAN is used only to send and receive EAPS messages.

The VLAN that will act as the control VLAN must be configured as follows:

- The VLAN must NOT be assigned an IP address, to avoid loops in the network.
- Only ring ports may be added as members of the control VLAN.
- The ring ports of the control VLAN must be tagged. This ensures that EAPS control VLAN traffic is serviced before any other traffic and that control VLAN messages reach their intended destinations.
- The control VLAN must be assigned a QoS profile of QP8 with the QoS profile priority setting `HighHi`.

A control VLAN cannot belong to more that one EAPS domain.

Adding a Control VLAN via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Choose a VLAN in `Control VLAN`. Click `Apply`.

Adding a Control VLAN via CLI

- The next example illustrates how to add a control VLAN via CLI.

Example 13-7. Adding a Control VLAN via CLI

```
DmSwitch3000#configure
DmSwitch3000(config)#interface vlan 10
DmSwitch3000(config-if-vlan-10)#exit
DmSwitch3000(config)#eaps datacom
DmSwitch3000(config)#eaps datacom control-vlan id 10
DmSwitch3000(config)#
```

13.8. Deleting a Control VLAN

Using the following command you will be able to delete a *control* VLAN.

Deleting a Control VLAN via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Choose `(none)` in `Control VLAN`. Click `Apply`.

Deleting a Control VLAN via CLI

- The next example illustrates how to delete a Control VLAN via CLI.

Example 13-8. Deleting a Control VLAN via CLI

```
DmSwitch3000(config)#no eaps datacom control-vlan
DmSwitch3000(config)#
```

13.9. Adding a Protected VLAN

You must configure one or more *protected* VLANs for each EAPS domain. The protected VLANs are the data-carrying VLANs.

When you configure the VLAN that will act as a protected VLAN, the ring ports of the protected VLAN must be tagged (except in the case of the default VLAN). As long as the ring is complete, the master node blocks the protected VLANs on its secondary port.

Adding a Protected VLAN via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Choose a VLAN ID in `Protected VLANs`. Click `Add`.

Adding a Protected VLAN via CLI

- The next example illustrates how to add a Protected VLAN via CLI.

Example 13-9. Adding a Protected VLAN via CLI

```
DmSwitch3000#configure
DmSwitch3000(config)#interface vlan 11
DmSwitch3000(config-if-vlan-11)#exit
DmSwitch3000(config)#eaps datacom protected-vlans id 11
DmSwitch3000(config)#interface vlan 12
DmSwitch3000(config-if-vlan-12)#exit
DmSwitch3000(config)#eaps datacom protected-vlans id 12
DmSwitch3000(config)#
```

13.10. Deleting a Protected VLAN

Using the following command you will be able to delete a *protected* VLAN.

Deleting a Protected VLAN via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Choose a VLAN ID in `Protected VLANs`. Click `Remove`.

Deleting a Protected VLAN via CLI

- The next example illustrates how to delete a Protected VLAN via CLI.

Example 13-10. Deleting a Protected VLAN via CLI

```
DmSwitch3000(config)#no eaps datacom protected-vlans id 11
DmSwitch3000(config)#
```

13.11. Configuring Failtime

Use the `failtime` keyword and its associated `seconds` parameter to specify the amount of time the master node waits before declaring a failed state and opens the logically blocked VLANs on the secondary port. `seconds` must be greater than the configured value for `hellotime`. The default value is three seconds.

Increasing the `failtime` value provides more protection against frequent "flapping" between the complete state and the failed state by waiting long enough to receive a health-check packet when the network is congested.

When the master node declared a failed state, it also flushes its forwarding database (FDB) and sends a "flush FDB" message to all the transit switches on the ring by way of the control VLAN. The reason for flushing the FDB is so that the switches can relearn the new directions to reach layer 2 end stations via the reconfigured topology.

Configuring Failtime via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Put the new value in `Fail timer interval` and click `Apply`.

Configuring Failtime via CLI

- The next example illustrates how to configure failtime via CLI.

Example 13-11. Configuring Failtime via CLI

```
DmSwitch3000(config)#eaps datacom failtime 5
DmSwitch3000(config)#
```

13.12. Configuring Hellotime

Use `hellotime` keyword and its associated `seconds` parameter to specify the amount of time the master node waits between transmissions of health-check packets on the control VLAN. Increasing the `hellotime` value keeps the processor from sending and processing too many health-check packets. Increasing the `hellotime` value should not affect the network convergence time, because transit nodes are already sending "link down" notifications.

This command applies only to the master node. If you configure the polling timers for a transit node, they will be ignored. If you later reconfigure that transit node as the master node, the polling timer values will be used as the current values.

Configuring Hellotime via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Put the new value in `Hello timer interval` and click `Apply`.

Configuring Hellotime via CLI

- The next example illustrates how to configure hellotime via CLI.

Example 13-12. Configuring Hellotime via CLI

```
DmSwitch3000(config)#eaps datacom hellotime 2
DmSwitch3000(config)#
```

13.13. Configuring EAPS Mode

Using the following command you will be able to set the EAPS mode of the node.

Configuring EAPS Mode via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Mark `Master` or `Transit` for Mode for the domain and click `Apply`.

Configuring EAPS Mode as Master via CLI

- The next example illustrates how to configure EAPS mode via CLI.

Example 13-13. Configuring EAPS Mode as Master via CLI

```
DmSwitch3000(config)#eaps datacom mode master
DmSwitch3000(config)#
```

Configuring EAPS Mode as Transit via CLI

- The next example illustrates how to configure EAPS mode via CLI.

Example 13-14. Configuring EAPS Mode as Transit via CLI

```
DmSwitch3000(config)#eaps datacom mode transit
DmSwitch3000(config)#
```

13.14. Configuring EAPS Port

Each node on the ring connects through two ring ports. One port must be configured as the *primary* port; the other must be configured as the *secondary* port.

Configuring EAPS Port via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. For both ports, select in `Primary Port` and `Secondary Port` the Unit and Port or Port-Channel. Click `Apply`.

Configuring EAPS Port via CLI

- The next example illustrates how to configure EAPS port via CLI.

Example 13-15. Configuring EAPS Port via CLI

```
DmSwitch3000(config)#eaps datacom port primary ethernet 15
DmSwitch3000(config)#eaps datacom port secondary ethernet 16
DmSwitch3000(config)#
```

13.15. Removing EAPS Port Configuration

Unconfiguring an EAPS port sets its internal configuration state to INVALID, which causes the port to appear in the Idle state with a port status of Unknown when you use the `show eaps detail` command to display the status information about the port.

Removing EAPS Port Configuration via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. For both ports, just select (none) for Port and Port-Channel in `Primary Port` or `Secondary Port` to remove the configuration.

Removing EAPS Port Configuration via CLI

- The next example illustrates how to remove EAPS Port configuration via CLI.

Example 13-16. Removing EAPS Port Configuration via CLI

```
DmSwitch3000(config)#no eaps datacom port primary
DmSwitch3000(config)#no eaps datacom port secondary
DmSwitch3000(config)#
```

13.16. Configuring EAPS Name

Using the following command you will be able to rename an existing EAPS domain.

Configuring EAPS Name via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the domain you want to configure. Mark `Rename the domain` and insert the new domain name in the text box.

Configuring EAPS Name via CLI

- The next example illustrates how to configure EAPS name via CLI.

Example 13-17. Configuring EAPS Name via CLI

```
DmSwitch3000(config)#eaps datacom name datacom2
DmSwitch3000(config)#
```

13.17. Displaying EAPS Summary

Displays EAPS domains and associated info such as Domain Name, Domain State, EAPS Mode, Enabled State, Control VLAN and VLAN ID and the Number of Protect VLANs in the domain. This is helpful when viewing the status info for large number of EAPS domains quickly.

Displaying EAPS Summary via CLI

- The next example illustrates how to Display EAPS Summary via CLI.

Example 13-18. Displaying EAPS Summary via CLI

```
DmSwitch3000(config)#show eaps

EAPS Enabled:         Yes

Domain           State           M   E   Pri   Sec   Ctrl   Protected#
---------------- --------------- --- --- ----- ----- ------ -----------
datacom          Idle            T   N   -     -     10     2

DmSwitch3000(config)#
```

13.18. Displaying EAPS Information

If you enter `show eaps` command without a keyword, the command displays less than with the `detail` keyword.

Use the optional domain name parameter to display status information for a specific EAPS domain.

The output displayed by this command depends on whether the node is a transit node or a master node. The display for a transit node contains information fields that are not shown for a master node. Also, some state values are different on a transit node than on a master node.

Displaying EAPS Information via Web

- Open `LAYER 2 - EAPS - EAPS Domain Configuration`. Select the Domain Name to see the configuration.

Displaying EAPS Information via CLI

- The next example illustrates how to display EAPS information via CLI.

Example 13-19. Displaying EAPS Information via CLI

```
DmSwitch3000(config)#show eaps detail

EAPS Enabled:         Yes

Domain Name:          datacom
State:                Idle
Enabled:              No               Mode:        Transit
```

```
Hello Timer interval: 1 sec
Fail Timer interval:  3 sec
Pre-forwarding Timer: 6 sec (learned)   Remaining:   0 sec
Last update from:     (none)
Primary port:         (not configured)
Secondary port:       (not configured)
Control VLAN ID:      10
Protected VLANs IDs:  11-12

DmSwitch3000(config)#
```

Chapter 14. Class of Service Configuration

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

14.1. Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and are sorted into the appropriate priority queue at the output port.

Command Usage

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queues blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

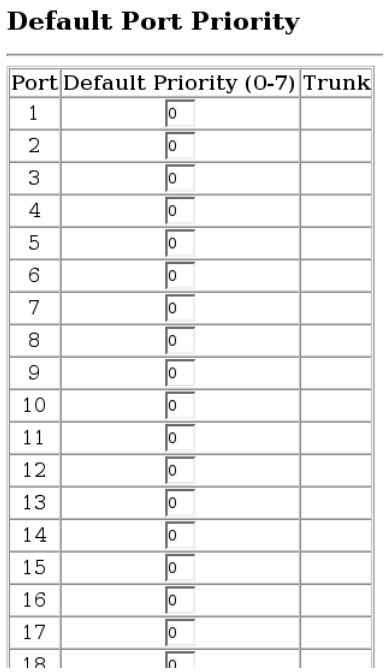
- `Default Priority` * - The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)
- `Number of Egress Traffic Classes` - The number of queue buffers provided for each port.

* CLI displays this information as "Priority for untagged traffic."

Setting the Default Port Priority via Web

- Open `Priority - Default Port Priority`, modify the default priority for any interface and then click Apply.

Figure 14-1. Setting the Default Port Priority via Web



Default Port Priority

Port	Default Priority (0-7)	Trunk
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	
11	0	
12	0	
13	0	
14	0	
15	0	
16	0	
17	0	
18	0	

Setting the Default Port Priority via CLI

- The next example show how to set the default port priority of 5 to port 2 via CLI.

Example 14-1. Setting the Default Port Priority via CLI

```
DmSwitch3000(config)#interface ethernet 1/2
DmSwitch3000(config-if-eth-1/2)#switchport priority default 5
DmSwitch3000(config-if-eth-1/2)#end
DmSwitch3000#show interfaces switchport ethernet 1/2
Information of Eth 1/2
 Broadcast threshold:           Enabled, 500 packets/second
 MTU:                           9198 bytes
 Ingress rate limit:            Disabled
 Egress rate limit:             Disabled
 Ingress Rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 5
 GVRP status:                   Disabled
 Protocol VLAN:
 Allowed VLAN:                  1(u)
 Forbidden VLAN:
 QinQ mode:                     External
 TPID:                          0x8100
DmSwitch3000#
```

14.2. Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on Strict Priority(SP), Round Robin (a exception of WRR), Weighted Round Robin (WRR) and Weighted Fair Queuing (WFQ). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 14-1. Mapping CoS Priority Values to Egress Queues

Queue	1	2	3	4	5	6	7	8
Priority	0	1	2	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Table 14-2. Priority Level Descriptions

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

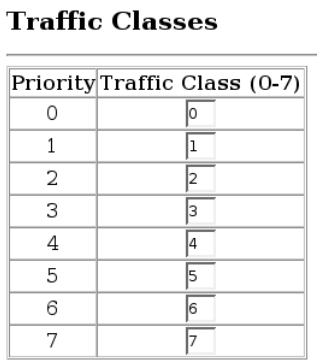
- `Priority` - CoS value. (Range: 0-7, where 7 is the highest priority)
- `Traffic Class` * - Output queue buffer. (Range: 1-8, where 8 is the highest CoS priority queue)

* CLI shows Queue ID.

Mapping CoS Values to Egress Queues via Web

- Open `Priority - Traffic Classes`. Assign priorities to the traffic classes and then click Apply.

Figure 14-2. Mapping CoS Values to Egress Queues via Web



Traffic Classes

Priority	Traffic Class (0-7)
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Mapping CoS Values to Egress Queues via CLI

- The next example shows how to change the CoS assignments via CLI.

Example 14-2. Mapping CoS Values to Egress Queues via CLI

```
DmSwitch3000(config)#qos cos-map 6 priority 2 3 4 5 6
DmSwitch3000#show qos cos-map
-------+-----------------+
 Queue | 802.1P Priority |
-------+-----------------+
   1   | 0               |
   2   | 1               |
   3   |                 |
   4   |                 |
   5   |                 |
   6   | 2 3 4 5 6       |
   7   |                 |
   8   | 7               |
-------+-----------------+
DmSwitch3000#
```

14.3. Selecting the Queue Mode

Once packets are mapped into CoS queues, they are forwarded depending upon the scheduling algorithm selected. The five possible configurations are:

- Strict Priority (SP)
- Round-Robin (RR)
- Weighted Round-Robin (WRR)
- Weighted Fair Queuing (WFQ)

- Combination Queuing:
  - SP + RR
  - SP + WRR
  - SP + WFQ

- `SP` - Strict Priority services the egress queues in sequential order. Any packets residing in the higher priority queues are transmitted first. Only when these queues are empty, packets of the next lower priority are allowed to be transmitted.
- `RR` - Round-Robin is a particular case from the Weighted Round-Robin mode (all the queues with weight one). In this configuration packets in each of the CoS queues have an equal opportunity to send packets. Even though several packets may be available in a higher-priority queue, it will only be allowed to send a packet after all the other queues get their chance.
- `WRR` - Weighted Round-Robin shares bandwidth at the egress ports by using the queue configured weights. All queues are programmed with weights according to desired packet distribution. The unit of the weights is one packet, not depending the packet size. The bandwidth distribution between two queues weighted by one and nine is not, necessarily, 10% and 90%. The distribution will be one packet to the first queue for nine packets to the second queue.
- `WFQ` - Weighted Fair Queuing scheduler mode provides a certain bandwidth minimum to all queues. Configured guaranteed bandwidth is first supplied per queue and any ramaining badwidth up to the configured maximum bandwidth is distributed in round-robin fashion.

In any schedule mode, one or more queues can be seted as strict priority queue (Combination Queuing). This queues always will have their packets transmitted first, until it get empty. After that others queues will have their chance according to the schedule mode rules.

Selecting the Queue Mode via CLI

- The next examples shows how to select the schedule mode via CLI.

Example 14-3. Selecting the WRR Schedule Mode via CLI

```
DmSwitch3000(config)#qos sched-mode wrr unit 1 ethernet 1to8 queue-weights 1
4 sp 2 6 8 sp 14
DmSwitch3000(config)#exit
DmSwitch3000(config)#show qos config ethernet 1/1
------+-------+------+--------+--------+--------+----------+-----------+
 PORT | QUEUE | MODE | MAX-BW | MIN-BW | WEIGHT | SP-QUEUE | WFQ-PRIOS |
------+-------+------+--------+--------+--------+----------+
 1/ 1 |   1   |  WRR | unlimi | ------ |    1   |    NO    |
 1/ 1 |   2   |  WRR | unlimi | ------ |    4   |    NO    |
 1/ 1 |   3   |  WRR | unlimi | ------ |    0   |    YES   |
 1/ 1 |   4   |  WRR | unlimi | ------ |    2   |    NO    |
 1/ 1 |   5   |  WRR | unlimi | ------ |    6   |    NO    |
 1/ 1 |   6   |  WRR | unlimi | ------ |    8   |    NO    |
 1/ 1 |   7   |  WRR | unlimi | ------ |    0   |    YES   |
 1/ 1 |   8   |  WRR | unlimi | ------ |   14   |    NO    |
------+-------+------+--------+--------+--------+----------+
```

```
DmSwitch3000(config)#
```

Example 14-4. Selecting the WFQ Schedule Mode via CLI

```
DmSwitch3000(config)#qos sched-mode wfq unit 1 ethernet 9to16 min-bw sp
2000 3000 4000 5000 sp 7000 8000
DmSwitch3000(config)#exit
DmSwitch3000(config)#show qos config ethernet 1/9
------+-------+------+--------+--------+--------+----------+
 PORT | QUEUE | MODE | MAX-BW | MIN-BW | WEIGHT | SP-QUEUE |
------+-------+------+--------+--------+--------+----------+
 1/ 9 |   1   |  WFQ | unlimi | ------ |   --   |    YES   |
 1/ 9 |   2   |  WFQ | unlimi |   2048 |   --   |    NO    |
 1/ 9 |   3   |  WFQ | unlimi |   3008 |   --   |    NO    |
 1/ 9 |   4   |  WFQ | unlimi |   4032 |   --   |    NO    |
 1/ 9 |   5   |  WFQ | unlimi |   5056 |   --   |    NO    |
 1/ 9 |   6   |  WFQ | unlimi | ------ |   --   |    YES   |
 1/ 9 |   7   |  WFQ | unlimi |   7040 |   --   |    NO    |
 1/ 9 |   8   |  WFQ | unlimi |   8000 |   --   |    NO    |
------+-------+------+--------+--------+--------+----------+
DmSwitch3000(config)#
```

14.4. Setting the Maximum Bandwidth for CoS Queues

This switch can limit the bandwidth in the egress port queues. This setting, unlike the port schedule mode that must be configured by groups, can assume diferentre values per port per queue. This value is always respected independent of the selected schedule mode or minimum bandwidth.

Setting the Maximum Bandwidth for CoS queues via CLI

- The next example shows how to set the maximum bandwidth to a port via CLI.

Example 14-5. Setting the Service Weight for Traffic Classes via CLI

```
DmSwitch3000(config)#qos max-bw 10000 unlimited 30000 40000 50000 60000
unlimited unlimited ethernet 1/20
DmSwitch3000(config)#exit
DmSwitch3000(config)#show qos config ethernet 20
------+-------+------+--------+--------+--------+----------+
 PORT | QUEUE | MODE | MAX-BW | MIN-BW | WEIGHT | SP-QUEUE |
------+-------+------+--------+--------+--------+----------+
 1/20 |   1   |  WRR |  10048 | ------ |    1   |    NO    |
 1/20 |   2   |  WRR | unlimi | ------ |    2   |    NO    |
 1/20 |   3   |  WRR |  30016 | ------ |    4   |    NO    |
 1/20 |   4   |  WRR |  40000 | ------ |    6   |    NO    |
 1/20 |   5   |  WRR |  50048 | ------ |    8   |    NO    |
 1/20 |   6   |  WRR |  60032 | ------ |   10   |    NO    |
 1/20 |   7   |  WRR | unlimi | ------ |   12   |    NO    |
 1/20 |   8   |  WRR | unlimi | ------ |   14   |    NO    |
------+-------+------+--------+--------+--------+----------+
DmSwitch3000#
```

14.5. Loading Auto-QoS Configuration

This switch uses the Strict Priority (SP) algorithm as the schedule mode of auto-QoS. Enabling auto-QoS, filters are created and CoS Precedences assigned based on DSCP label on the ingress packets to reproduce in the egress queues a behavior as described in the following table.

Table 14-3. Traffic Types, Packet Labels and Egress Queues

Traffic Flow	DSCP	CoS Precedence	Egress Queue
STP BPDU	56	7	7
Routing Protocol	48	6	6
VoIP Data	46	5	5
Real-Time Video	32	4	4
VoIP Control	24, 26	3	3
All Other	-	2, 1, 0	2, 1, 0

Enabling Auto-QoS via CLI

- The next example shows how to load the Auto-QoS configuration via CLI.

Example 14-6. Enabling Auto-QoS via CLI

```
DmSwitch3000(config)#queue auto-qos
DmSwitch3000(config)#filter new remark auto_qos match dscp 0 action 802.1p 0
ingress ethernet all priority 14
 Filter 1 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 8 action 802.1p 1
ingress ethernet all priority 14
 Filter 2 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 16 action 802.1p 2
ingress ethernet all priority 14
 Filter 3 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 24 action 802.1p 3
ingress ethernet all priority 14
 Filter 4 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 26 action 802.1p 3
ingress ethernet all priority 14
 Filter 5 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 32 action 802.1p 4
ingress ethernet all priority 14
 Filter 6 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 46 action 802.1p 5
ingress ethernet all priority 14
 Filter 7 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 48 action 802.1p 6
ingress ethernet all priority 14
 Filter 8 created.
DmSwitch3000(config)#filter new remark auto_qos match dscp 56 action 802.1p 7
ingress ethernet all priority 14
 Filter 9 created.
DmSwitch3000(config)#queue cos-map 0 0
DmSwitch3000(config)#queue cos-map 1 1
DmSwitch3000(config)#queue cos-map 2 2
DmSwitch3000(config)#queue cos-map 3 3
DmSwitch3000(config)#queue cos-map 4 4
```

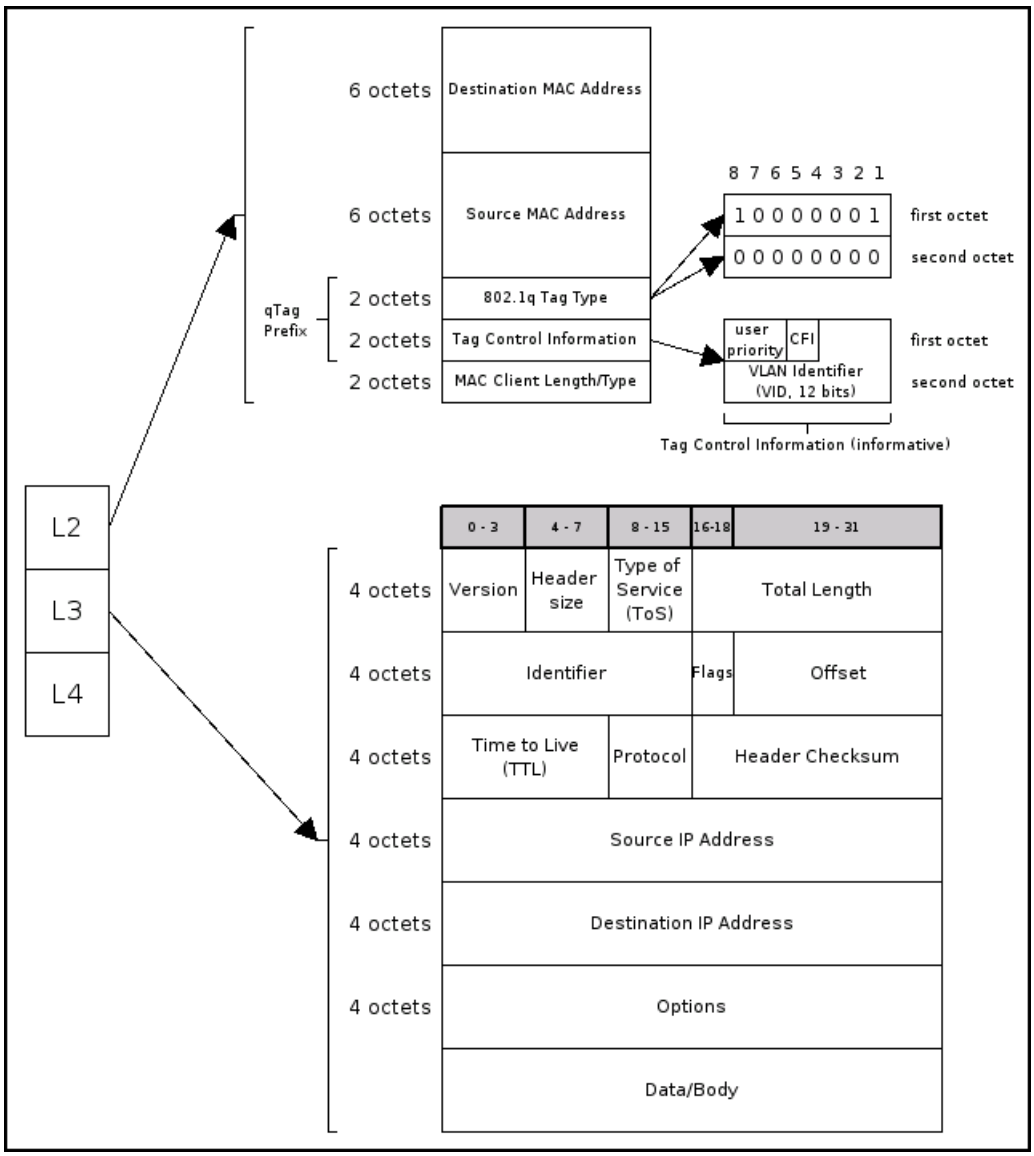
```
DmSwitch3000(config)#queue cos-map 5 5
DmSwitch3000(config)#queue cos-map 6 6
DmSwitch3000(config)#queue cos-map 7 7
DmSwitch3000(config)#queue mode strict
DmSwitch3000(config)#queue auto-qos
DmSwitch3000#
```

Chapter 15. Packet Filters

In this chapter will be shown how to create packet filters. Some examples will be given showing that are more than one way to create the same filter because some parameters have no order of precedence. This chapter purpose is to give you an overview of what can be done to control packet flow through the switch.

Note: This switch can work with at most 1280 filters.

Figure 15-1. This figure gives an idea of the protocol parts that are analysed by the filters.



15.1. Displaying Filter Information

Command Attributes

- `Action Type` - Show filters by action type.
- `Monitor` - Show filters with monitoring actions.
- `QoS` - Show filters with QoS actions.

- `Security` - Show filters with security actions.
- `VLAN` - Show filters with VLAN actions.
- `Ingress` - Show filters by ingress port.
- `ID` - Show filter selecting by their ID.
- `Sort Remark` - Show filters sorted by their remark.
- `State` - Show filters enabled or disabled.

Displaying Filter Information via CLI

- The next example shows a few commands used to display filter information via CLI.

Example 15-1. Displaying Filter Information via CLI

```
DmSwitch3000#show filter action-type monitor
 Filter 7: enabled, priority 8
   Actions:     monitor
   Matches:     All packets
   Ingress:

 Filter 33: enabled, priority 8
   Actions:     monitor
   Matches:     All packets
   Ingress:     Eth1/10

DmSwitch3000#show filter action-type qos
 Filter 10: enabled, priority 8
   Actions:     802.1p 2
   Matches:     All packets
   Ingress:

 Filter 15: disabled, priority 8
   Actions:     802.1p-from-tos
   Matches:     All packets
   Ingress:

 Filter 17: disabled, priority 8
   Actions:     drop-precedence
   Matches:     All packets
   Ingress:

DmSwitch3000#show filter action-type security
 Filter 49: enabled, priority 8
   Actions:     permit
   Matches:     source-ip 192.168.10.0 255.255.255.0
   Ingress:

 Filter 50: enabled, priority 8
   Actions:     permit
   Matches:     source-mac 00-01-00-00-01-00 00-FF-00-00-FF-00
   Ingress:

 Filter 51: enabled, priority 8
   Actions:     permit
   Matches:     source-port 22
   Ingress:

DmSwitch3000#show filter action-type vlan
 Filter 29: disabled, priority 8
   Actions:     vlan 5
   Matches:     All packets
```

```
   Ingress:

DmSwitch3000#show filter id 20
 Filter 20: disabled, priority 8
   Actions:     dscp 60
   Matches:     All packets
   Ingress:

DmSwitch3000#show filter ingress ethernet 10
 Filter 31: enabled, priority 8
   Actions:     deny
   Matches:     All packets
   Ingress:     Eth1/10

DmSwitch3000#show filter state disabled
 Filter 9: disabled, priority 8
   Actions:     monitor
   Matches:     All packets
   Ingress:

 Filter 12: disabled, priority 8
   Actions:     802.1p 2
   Matches:     All packets
   Ingress:

DmSwitch3000#
```

15.2. Creating and Editing Filters

Command Attributes

- `New` - Creates a new filter.
- `ID` - Selects a filter to edit by its ID.

15.2.1. Filter Matching

Command Attributes

- `802.1p` - Make the switch find matches by 802.1p priority.
- `All` - Matches all traffic. (Default option for new filters)
- `Destination IP` - Find matches by packet destination IP address.
- `Destionation MAC` - Find matches by packet destination MAC address.
- `Destionation Port` - Find matches by packet destination Port.
- `DSCP` - Matches by IP DSCP field.
- `Ethertype` - Selects packets by EtherType field.
- `Protocol` - Matches by L4 protocol from IP type field.
- `Source IP` - Find matches by packet source IP address.
- `Source MAC` - Find matches by packet source MAC address.

- `Source Port` - Find matches by packet source Port.
- `ToS Bits` - Selects packets by IP ToS lower bits value.
- `ToS Precedence` - Matches by IP ToS Precedence.
- `VLAN` - The switch will find matches based on the VLAN ID specified.

15.2.1.1. Matching by 802.1p priority value

Creating a filter via CLI which matches packets with 802.1p priority

- The next example show how to create a filter via CLI which matches packets with 802.1p priority.

Example 15-2. Creating a filter via CLI which matches packets with 802.1p priority.

```
DmSwitch3000(config)#filter new match 802.1p 3 action permit
 Filter 1 created.
DmSwitch3000(config)#
```

15.2.1.2. Matching all packets

Creating a filter via CLI which matches all packets

- The next example show how to create a filter via CLI which matches all packets.

Example 15-3. Creating a filter via CLI which matches all packets.

```
DmSwitch3000(config)#filter new match all action permit
 Filter 2 created.
DmSwitch3000(config)#
```

15.2.1.3. Matching by destination IP

Creating a filter via CLI which matches packets by their destination/source IP

- The next example show how to create a filter via CLI which matches packets by their destination IP.

Example 15-4. Creating a filter via CLI which matches packets by their destination IP.

```
DmSwitch3000(config)#filter new match destination-ip 192.168.10.0 255.255.255.0 action permit
 Filter 3 created.
DmSwitch3000(config)#
```

15.2.1.4. Matching by destination/source MAC address

Creating a filter via CLI which matches packets by their destination MAC address

- The next example show how to create a filter via CLI which matches packets by their destination MAC address. Followed by the MAC address, a bitmask must be supplied. In this example, all traffic from the products of DATACOM manufacturer (00-04-DF) will be accepted by the switch.

Example 15-5. Matching by destination MAC address.

```
DmSwitch3000(config)#filter new match source-mac 00-04-DF-00-00-00 FF-FF-FF-00-00-00
action permit ingress ethernet all
 Filter 4 created.
DmSwitch3000(config)#
```

15.2.1.5. Matching by destination/source port

Creating a filter via CLI which matches packets by their destination port

- The next example show how to create a filter via CLI which matches packets by their destination port.

Example 15-6. Creating a filter via CLI which matches packets by their destination port.

```
DmSwitch3000(config)#filter new match destination-port 0-22 action permit
 Filter 5 created.
DmSwitch3000(config)#
```

15.2.1.6. Matching by IP DSCP field

Creating a filter via CLI which matches packets by their IP DSCP field

- The next example show how to create a filter via CLI which matches packets by their IP DSCP field

Example 15-7. Creating a filter via CLI which matches packets by their IP DSCP field

```
DmSwitch3000(config)#filter new match dscp 60 action permit
 Filter 6 created.
DmSwitch3000(config)#
```

15.2.1.7. Selecting packets by EtherType field

Creating a filter via CLI that selects packets by EtherType field

- The next example show how to create a filter via CLI that selects packets by EtherType field. This filter permits IPv6 (0x86DD) traffic.

Example 15-8. Creating a filter via CLI that selects packets by EtherType field.

```
DmSwitch3000(config)#filter new match ethertype 0x86DD action permit
 Filter 7 created.
DmSwitch3000(config)#
```

15.2.1.8. Matching by L4 protocol

Creating a filter via CLI that matches by L4 protocol

- The next example show how to create a filter via CLI that matches by L4 protocol. In this filter, the IP type field will be used to match.

Example 15-9. Creating a filter via CLI that matches by L4 protocol.

```
DmSwitch3000(config)#filter new match protocol 22 action permit
 Filter 8 created.
DmSwitch3000(config)#
```

15.2.1.9. Selecting packets by IP ToS lower bits

Creating a filter via CLI that selects packets by IP ToS lower bits

- The next example show how to create a filter via CLI that selects packets by its IP ToS lower bits with value 12.

Example 15-10. Creating a filter via CLI that selects packets by IP ToS lower bits.

```
DmSwitch3000(config)#filter new match tos-bits 12 action permit
 Filter 9 created.
DmSwitch3000(config)#
```

15.2.1.10. Matching by IP ToS Precedence

Creating a filter via CLI that matches packets by IP ToS Precedence

- The next example show how to create a filter via CLI that matches packets by IP ToS Precedence.

Example 15-11. Creating a filter via CLI that matches packets by IP ToS Precedence.

```
DmSwitch3000(config)#filter new match tos-precedence 5 action permit
 Filter 10 created.
DmSwitch3000(config)#
```

15.2.1.11. Selecting traffic by packet VLAN ID

Creating a filter via CLI which selects traffic by packet VLAN ID

- The next example show how to create a filter via CLI which selects traffic by packet VLAN ID.

Example 15-12. Creating a filter via CLI which selects traffic by packet VLAN ID.

```
DmSwitch3000(config)#filter new match vlan 5 action permit
 Filter 11 created.
DmSwitch3000(config)#
```

15.2.2. Filtering Actions

Command Attributes

- `Permit` - Gives permission for some kind of traffic.
- `Deny` - Denies traffic.
- `Monitor` - Monitors packets.
- `802.1p` - Sets a 802.1p priority value.
- `802.1p from ToS` - Sets a 802.1p priority from IP ToS Precedence.
- `Drop Precedence` - Internally sets packet drop precedence.
- `DSCP` - Sets Differentiated Services Code Point.
- `ToS` - Sets IP ToS Precedence value.
- `ToS from 802.1p` - Sets IP ToS Precedence from 802.1p priority.
- `VLAN` - Sets the defined VLAN ID to the packet.

15.2.2.1. Giving Permission

Creating a filter via CLI that gives permission

- The next example show how to create a filter via CLI that gives permission.

Example 15-13. Creating a filter via CLI that gives permission.

```
DmSwitch3000(config)#filter new match destination-ip 192.168.200.254 255.255.255.0 action
permit
 Filter 12 created.
DmSwitch3000(config)#
```

is the same as

```
DmSwitch3000(config)#filter new enable match destination-ip 192.168.200.254 255.255.255.0
action permit
 Filter 12 created.
DmSwitch3000(config)#
```

and you can create it disabled with the following command

```
DmSwitch3000(config)#filter new disable match destination-ip 192.168.200.254 255.255.255.0
action permit
 Filter 12 created.
DmSwitch3000(config)#
```

15.2.2.2. Revoking Access

Creating a filter via CLI that denies traffic

- The next example show how to create a filter via CLI that denies traffic.

Example 15-14. Creating a filter via CLI that denies traffic.

```
DmSwitch3000(config)#filter new match 802.1p 3 action deny
 Filter 13 created.
DmSwitch3000(config)#
```

15.2.2.3. Monitoring Traffic

Creating a filter via CLI to monitor traffic

- The next example show how to create a filter via CLI to monitor traffic. In this example, packets coming from ethernet 1 will me monitored to ethernet 12.

Example 15-15. Creating a filter via CLI to monitor traffic

```
zmSwitch3000(config)#filter new action monitor ingress ethernet 1
 Filter 14 created.
DmSwitch3000(config)#monitor destination 12
DmSwitch3000(config)#
```

15.2.2.4. Setting 802.1p Priority Value

Creating a filter via CLI with a 802.1p priority value

- The next example show how to create a filter via CLI with a 802.1p priority value.

Example 15-16. Creating a filter via CLI with a 802.1p priority value.

```
DmSwitch3000(config)#filter match ethertype 0x0800 action 802.1p 2
 Filter 15 created.
DmSwitch3000(config)#
```

15.2.2.5. Setting 802.1p Priority from IP ToS Precedence

Creating a filter via CLI with a 802.1p priority from IP ToS Precedence

- The next example show how to create a filter via CLI which sets the 802.1p priority value derived from the IP ToS Precedence table.

Example 15-17. Creating a filter via CLI with a 802.1p priority from IP ToS Precedence.

```
DmSwitch3000(config)#filter new match destination-port 22 action 802.1p-from-tos
 Filter 16 created.
DmSwitch3000(config)#
```

15.2.2.6. Dropping Precedence

Creating a filter via CLI for packet drop precedence

- The next example show how to create a filter via CLI for packet drop precedence.

Example 15-18. Creating a filter via CLI for packet drop precedence.

```
DmSwitch3000(config)#filter match dscp 33 new action drop-precedence
 Filter 17 created.
DmSwitch3000(config)#
```

15.2.2.7. Setting Differentiated Services Code Point

Creating a filter via CLI with Differentiated Services Code Point

- The next example show how to create a filter via CLI with Differentiated Services Code Point.

Example 15-19. Creating a filter via CLI with Differentiated Services Code Point.

```
DmSwitch3000(config)#filter new match protocol tcp action dscp 60
 Filter 18 created.
DmSwitch3000(config)#
```

15.2.2.8. Setting IP ToS Precedence value

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

Table 15-1. Mapping IP Precedence

Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

Creating a filter via CLI with IP ToS Precedence value

- The next example show how to create a filter via CLI with IP ToS Precedence value.

Example 15-20. Creating a filter via CLI with IP ToS Precedence value.

```
DmSwitch3000(config)#filter new match source-port 80 action tos 2
 Filter 19 created.
DmSwitch3000(config)#
```

15.2.2.9. Setting IP ToS Precedence from 802.1p Priority

Creating a filter via CLI with IP ToS Precedence from 802.1p priority

- The next example show how to creating a filter via CLI with IP ToS Precedence from 802.1p priority.

Example 15-21. Creating a filter via CLI with IP ToS Precedence from 802.1p priority.

```
DmSwitch3000(config)#filter new match 802.1p 1 action tos-from-802.1p
 Filter 20 created.
DmSwitch3000(config)#
```

15.2.2.10. Setting a VLAN ID to a packet

Creating a filter via CLI that sets packet VLAN ID

- The next example show how to create a filter via CLI that sets packet VLAN ID.

Example 15-22. Creating a filter via CLI that sets packet VLAN ID.

```
DmSwitch3000(config)#filter new match vlan 2 action vlan 5
 Filter 21 created.
DmSwitch3000(config)#
```

15.2.3. Filtering Ingress

Command Attributes

- `Ingress Ethernet` - Defines from where the packets will come. (Default: none)

Creating a filter via CLI that gives permission to a packet selecting it by its ingress port

- The next example show how to create a filter via CLI that allows packets coming from ethernet 10.

Example 15-23. Creating a filter via CLI that selects packets by its ingress port.

```
DmSwitch3000(config)#filter new action permit ingress ethernet 10
 Filter 22 created.
DmSwitch3000(config)#
```

Creating a filter via CLI that denies packets coming from a defined port

- The next example show how to create a filter via CLI that denies packets coming from ethernet 10.

Example 15-24. Creating a filter via CLI that selects packets by its ingress port.

```
DmSwitch3000(config)#filter new action deny ingress ethernet 10
 Filter 23 created.
DmSwitch3000(config)#
```

15.2.4. Remarked Filters

Command Attributes

- `Remark` - Adds a remark or a descriptive text to the filter.

Creating a remarked filter via CLI

- The next example show how to create a remarked filter via CLI.

Example 15-25. Creating a remarked filter via CLI

```
DmSwitch3000(config)#filter new remark my_new_filter action permit
 Filter 24 created.
DmSwitch3000(config)#
```

15.2.5. Setting Priorities to Filters

The act of setting priorities is basically used to solve problems with filters with the same matches and conflicting actions. For example, if you have two filters with matches for an IP packet with actions of

deny and permit respectively then the only the filter with the higher priority will be applied. The range of priorities varies between 0 and 14 and the higher value the higher will be the priority set to the filter.

Command Attributes

- `Priority` - Adds a priority to a filter.

Creating filters via CLI and setting their priority

- The next example show how to solve problems between filters with conflicting actions. The first created filter will permit all traffic based on the IP protocol to be forwarded. The second filter will deny traffic with IP destination address 192.168.0.1. A packet with this IP destination will match both filters and there will be two conflicting actions for this packet. In this example, the conflict is solved by setting priorities to these filters. The actions within the filter with the highest priority will be applied to this packet.

  Example 15-26. Creating a filter with a priority set via CLI

```
DmSwitch3000(config)#filter new match ethertype 0x0800 action permit
 Filter 25 created.
DmSwitch3000(config)#filter new match destination-ip 192.168.0.1 255.255.255.255 action deny
 Filter 26 created.
DmSwitch3000(config)#
DmSwitch3000(config)#filter 4 priority 12
DmSwitch3000(config)#filter 3 priority 10
DmSwitch3000(config)#
```

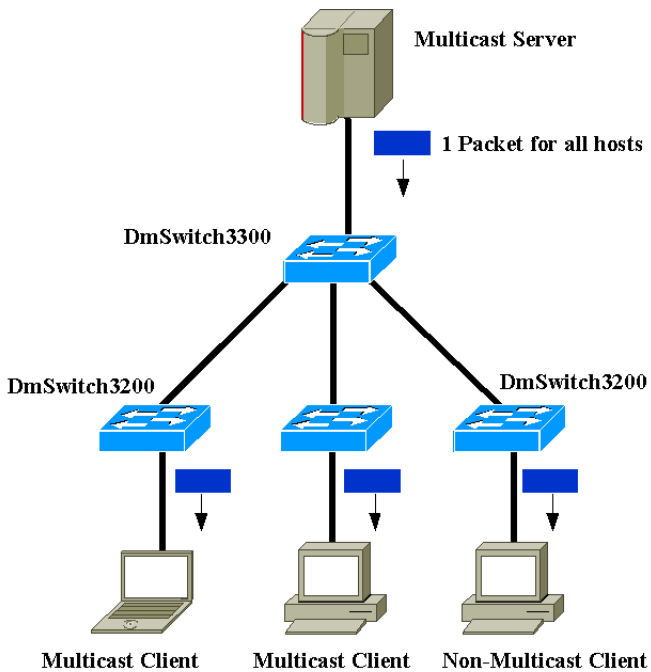
Chapter 16. IGMP

This chapter describes the advantages of using multicast and how to configure *Internet Group Management Protocol* (IGMP) snooping and query on the DmSwitch3000.

Multicast is a feature that allows a more efficient use of real-time applications such as streaming video or videoconferecing on the network. There are typically three types of transmission techniques used to implement this kind of applications: broadcast, unicast and multicast.

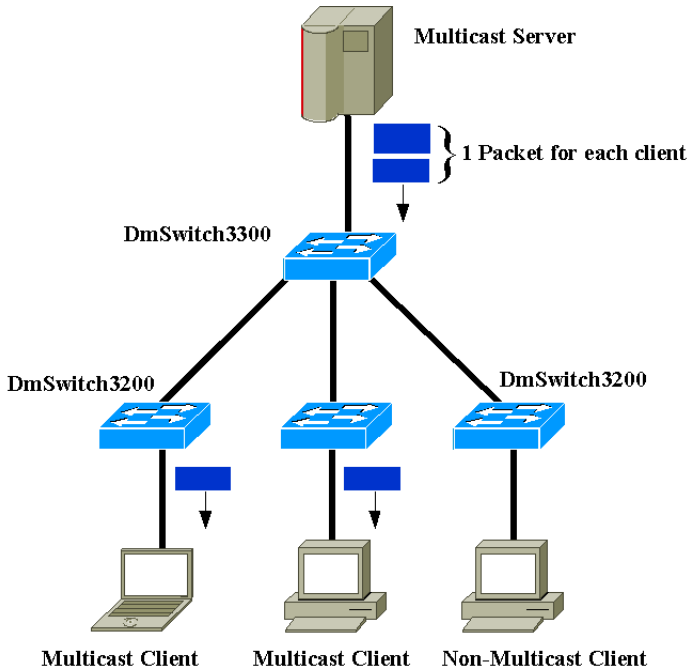
In the broadcast scenario, the streaming server sends only one copy of the stream to all hosts on the network. In this case, traffic will be sent even to clients that are not interested in receiving the data stream, generating waste of bandwidth.

Figure 16-1. Broadcast Traffic



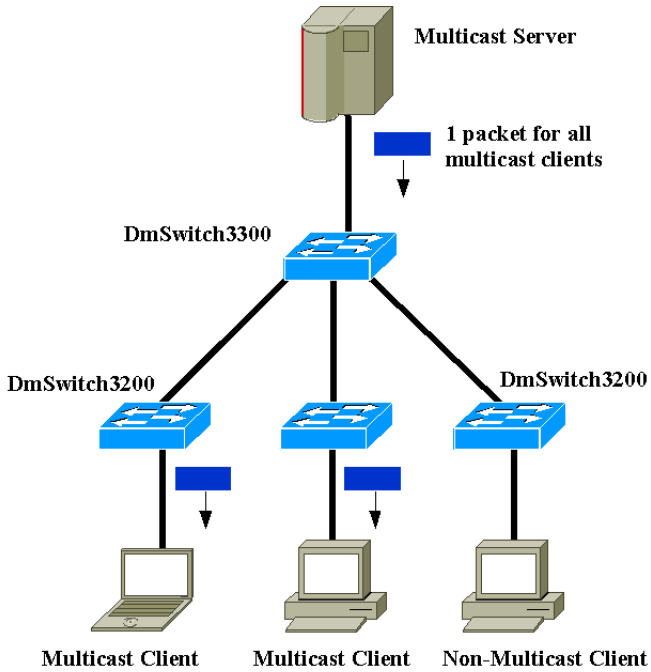
In the unicast scenario, we usually have a streaming server that sends packets to all desired clients on the network. In this case, multiple copies of the same data streaming are sent separately from the server to each client. Note that this approach leads to a traffic overload on the server link as the number of clients grows.

Figure 16-2. Replicated Unicast Traffic



In the multicast scenario, the streaming server does not have to establish a separate connection with each client, it simply registers its multicast service with the local switch and starts to send the data stream. The clients equally register with the local switch or router its multicast group and start to receive the data stream. IGMP can be used in order to do the registration task on the network.

Figure 16-3. Multicast Traffic



The IGMP snooping feature allows the switch to snoop on multicast group membership reports sent by multicast clients and servers to the multicast router, so it can forward traffic only to the registered interfaces, alleviating the load on the server link and improving the overall network performance.

If there is no multicast routing on other router/switches in the network, this switch can also act as an IGMP Snooping and Querier, in order to actively discover multicast clients on the network and establish an efficient multicast topology. Acting as a querier, the switch sends IGMP queries in order to discover where are the multicast clients. A static IGMP router interface can also be configured on a port, indicating the presence of a multicast router/switch querier on the network. Static multicast entries can also be entered, allowing a more strict control over the multicast registration procedure.

This switch supports the following IGMP features:

- IGMP versions 1, 2 and 3
- IGMP Snooping
- IGMP Snooping and Querier

16.1. Configuring IGMP

This switch can be configured to snoop IGMP membership report messages. You can additionally configure it to act as a IGMP querier. Use the querier option when there is no other querier on the network or when using a backup querier scheme.

16.1.1. Configuring IGMP Snooping and Querier

Command Attributes

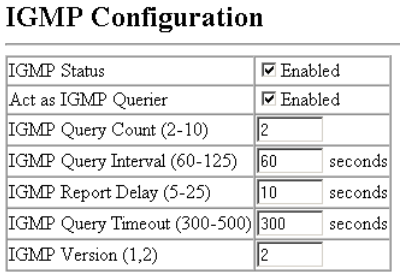
- `IGMP Status` - Enables/Disables the IGMP Snooping option on the switch.
- `Querier Status` - Choose if the switch will act as a IGMP Snooping and Querier.
- `IGMP Query Count (2-10)` - Sets the number of queries without response the switch waits before removing the multicast entries from its forwarding table.
- `IGMP Query Interval (60-125)` - Sets the time interval between sending queries.
- `IGMP Report Delay (5-25)` - Set the maximum response time a host waits before replying with a membership report to a querier.
- `IGMP Query Timeout (300-500)` - Sets the time interval the switch waits for a query before removing the mrouter entry from its forwarding table.
- `IGMP Version(1,2,3)` - Sets the IGMP version used by the switch.
- `IGMP Query IP Address` - Sets the IP address used by the switch when sending IGMP queries.

* *Note: In some cases where more than one switch is configured as querier on the network, the switch with the lowest IP address will be elected as querier. When the IGMP IP is not configured, the switch will use the first available IP from its IP interfaces. IGMP querier functions will not work without a source IP address.*

IGMP Snooping and Querier Configuration via Web

- Open `IGMP Snooping - IGMP Configuration`, choose the IGMP mode (stand-alone snooping or snooping and querier) fill in the desired timers values and version. Click `Apply` to commit.

Figure 16-4. Configuring IGMP Snooping and Querier via Web



IGMP Configuration via CLI

- The next example configures the switch to use IGMP version 2 acting as a querier with an IP address of 192.168.10.1

Example 16-1. Configuring IGMP Snooping and Querier via CLI

```
DmSwitch3000(config)#ip igmp snooping version 2
DmSwitch3000(config)#ip igmp snooping
DmSwitch3000(config)#ip igmp snooping querier
DmSwitch3000(config)#ip igmp snooping ip 192.168.10.1
DmSwitch3000(config)#
```

16.1.2. Configuring IGMP Static Entries

In order to ensure that a multicast router or multicast group will be permanently registered on the switch, you can configure static entries on the interfaces connected to routers or multicast clients. By doing this, every port configured and connected to a multicast router will register all the multicast groups inside the corresponding VLAN. This means that every membership report will be forwarded to the multicast router, so it will be able to forward multicast traffic properly.

By configuring a static multicast IP entry on an interface, the switch will always forward multicast traffic for this group on this port, independently on the reception of membership reports for this group.

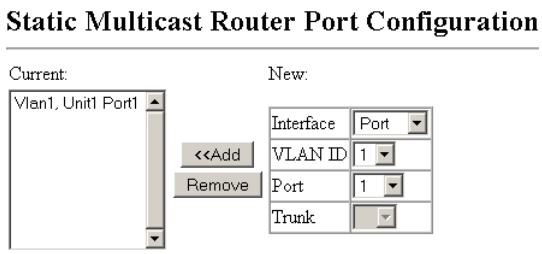
Command Attributes

- `Interface` - Selects whether a port or a port-channel will be configured.
- `VLAN ID` - Choose the VLAN that will propagate the multicast traffic for this entry.
- `Port` or `Port-Channel` - Selects the interface that will be attached to a multicast router or multicast group.
- `Multicast IP Address` - Sets the group multicast IP address that will be registered on the interface.

Configuring IGMP Static Multicast Router Port via Web

- Open `IGMP Snooping - Static Multicast Router Port Configuration` , select an interface and VLAN on wich the multicast router is connected. Click `Apply` to commit.

Figure 16-5. Configuring IGMP Static Multicast Router Port via Web



Configuring IGMP Static Multicast Router Port via CLI

- The next example configures a static multicast router entry on VLAN1, switch interface ethernet 1/1.

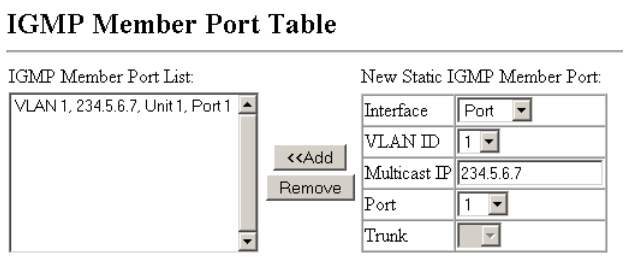
Example 16-2. Configuring IGMP Static Multicast Router Port via CLI

```
DmSwitch3000(config)#ip igmp snooping vlan 1 mroute ethernet 1
DmSwitch3000(config)#
```

Configuring IGMP Static Multicast Group via Web

- Open `IGMP Snooping - IGMP Member Port Table` , select an interface, VLAN and set an IP multicast address to be registered. Click `Apply` to commit.

Figure 16-6. Configuring IGMP Static Multicast Group via Web



Configuring IGMP Static Multicast Group via CLI

- The next example configures the switch to statically register the multicast group IP address 234.5.6.7 in the VLAN 1, interface ethernet 1/1.

Example 16-3. Configuring IGMP Static Multicast Group via CLI

```
DmSwitch3000(config)#ip igmp snooping vlan 1 static 234.5.6.7 ethernet 1
DmSwitch3000(config)#
```

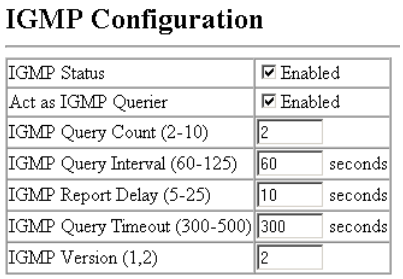
16.1.3. Displaying IGMP Information

16.1.3.1. Displaying IGMP Global Information

Displaying IGMP Global Information via Web

- Open `IGMP Snooping - IGMP Configuration`

Figure 16-7. Displaying IGMP Global Information via Web



Displaying IGMP Global Information via CLI

- The next example illustrates how to display IGMP configuration parameters via CLI.

Example 16-4. Displaying IGMP Global Information via CLI:

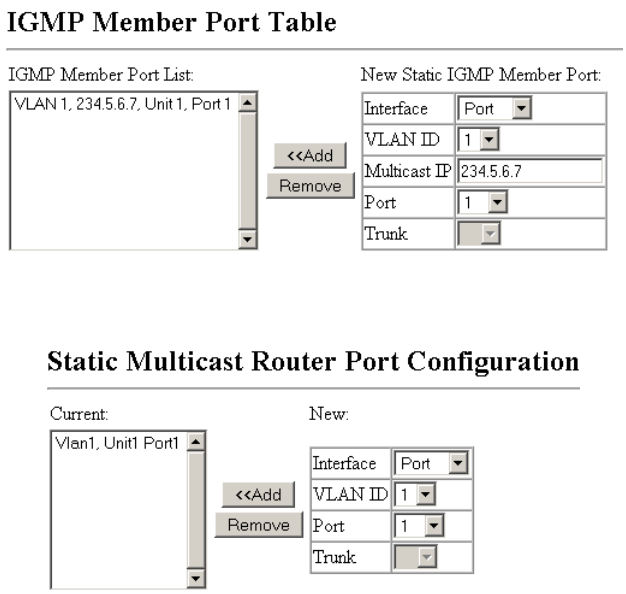
```
DmSwitch3000#show ip igmp snooping
Service status:             Enabled
Querier status:             Enabled
Query count:                2
Query interval:             60 sec
Query max response time:    10 sec
Router port expire time:    300 sec
IGMP snooping version:      2
DmSwitch3000#
```

16.1.3.2. Displaying IGMP Static Information

Displaying IGMP Static Information via Web

- Open `IGMP Snooping - Static Multicast Router Port Configuration` or `IGMP Snooping - IGMP Member Port Table`.

Figure 16-8. Displaying IGMP Static Information via Web



Displaying IGMP Static Information via CLI

- The next example illustrates how to display IGMP Static Information via CLI.

Example 16-5. Displaying IGMP Static Information via CLI

```
DmSwitch3000(config)#show ip igmp snooping mroute
VLAN M'cast Router Ports Type
---- ------------------- -------
   1            Eth1/ 1 Static
DmSwitch3000#
DmSwitch3000#show mac-address-table multicast
VLAN M'cast IP addr. Member ports Type
---- --------------- ------------ -------
   1       234.5.6.7      Eth1/ 2 Static
DmSwitch3000#
```

Chapter 17. Static Routing

This switch provides wire-speed layer 3 (IP) routing. It can work with static routes, and it can also exchange information with others routers on the network using RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) protocols, dynamically building and maintaining its routing table.

This chapter will focus on static routing only.

17.1. Router Interfaces

The switch routes packets between router interfaces. A router interface is simply a VLAN that has an IP address assigned to it.

17.2. Static Routes

Static routes are manually entered into the routing table. They can be used to reach networks not advertised by routers, or in simple configurations where it is not desirable to run routing protocols.

Command Attributes

- `Subnet` - Network subnet (IP address/prefix length).
- `Gateway` - IP address of gateway.

Static Route Configuration via CLI

- The next example creates two VLANs, with IPs 192.168.1.1 and 192.168.2.1, configures a static route to reach 192.168.3.0/24 network via a gateway with IP address 192.168.1.10, and dumps the result:

Example 17-1. Adding Static Route via CLI

```
DmSwitch3000#configure
DmSwitch3000(config)#interface vlan 10
DmSwitch3000(config-if-vlan-10)#ip address 192.168.1.1/24
DmSwitch3000(config-if-vlan-10)#set-member untagged ethernet range 1 12
DmSwitch3000(config-if-vlan-10)#interface vlan 20
DmSwitch3000(config-if-vlan-20)#ip address 192.168.2.1/24
DmSwitch3000(config-if-vlan-20)#set-member untagged ethernet range 13 24
DmSwitch3000(config-if-vlan-20)#interface ethernet range 1 12
DmSwitch3000(config-if-eth-1/1-to-1/12)#switchport native vlan 10
DmSwitch3000(config-if-eth-1/1-to-1/12)#interface ethernet range 13 24
DmSwitch3000(config-if-eth-1/13-to-1/24)#switchport native vlan 20
DmSwitch3000(config-if-eth-1/13-to-1/24)#exit
DmSwitch3000(config)#ip route 192.168.3.0/24 192.168.1.10
DmSwitch3000(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF
```

```
C 127.0.0.0/8 is directly connected, loopback
C 192.168.1.0/24 is directly connected, vlan 10
C 192.168.2.0/24 is directly connected, vlan 20
S 192.168.3.0/24 [1/0] via 192.168.1.10, vlan 10
DmSwitch3000(config)#
```

- The route can be removed adding **no** to the beggining of the command:

Example 17-2. Removing Static Route via CLI

```
DmSwitch3000(config)#no ip route 192.168.3.0/24 192.168.1.10
DmSwitch3000(config)#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF

C 127.0.0.0/8 is directly connected, loopback
C 192.168.1.0/24 is directly connected, vlan 10
C 192.168.2.0/24 is directly connected, vlan 20
DmSwitch3000(config)#
```

17.3. Hardware Tables

In this switch routing is done by hardware, using two tables:

Hardware Tables

- A host table, which maps directly connected hosts' IP addresses to MAC/VLAN/Port.
- A longest prefix match (LPM) table, which maps subnets to gateway MAC/VLAN/Port.

Checking Hardware Tables via CLI

- These tables are mantained by the firmware running on the equipment, but their state can be checked with the commands below:

Example 17-3. Checking Hardware Tables via CLI

```
DmSwitch3000#show ip hardware host-table
IP address       MAC               VLAN  Port  Hit
---------------  ----------------  ----  ----  ---
192.168.1.10     00:04:DF:00:01:10  10    2     Y
192.168.2.10     00:04:DF:00:59:D7  20    14    Y
255.255.255.255  00:00:00:00:00:00  0     1     N

Total: 3         Free: 4093


DmSwitch3000#show ip hardware lpm-table
Network address  Next Hop MAC       VLAN  Port  Hit
---------------  ----------------  ----  ----  ---
192.168.3.0      00:04:DF:00:01:10  10    2     N

Total: 1         Free: 16384
DmSwitch3000#
```