SRstackware® Intelligent Network Software

Layer 2 Configuration Guide

P/N: 6806800N86E

April 2020

SMART™ Embedded Computing

Trademarks

The stylized "S" and "SMART" is a registered trademark of SMART Modular Technologies, Inc. and “SMART Embedded Computing” and the SMART Embedded Computing logo are trademarks of SMART Modular Technologies, Inc. All other names and logos referred to are trade names, trademarks, or registered trademarks of their respective owners. These materials are provided by SMART Embedded Computing as a service to its customers and may be used for informational purposes only.

Disclaimer*

SMART Embedded Computing (SMART EC) assumes no responsibility for errors or omissions in these materials. **These materials are provided "AS IS" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.** SMART EC further does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SMART EC shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. SMART EC may make changes to these materials, or to the products described therein, at any time without notice. SMART EC makes no commitment to update the information contained within these materials.

Electronic versions of this material may be read online, downloaded for personal use, or referenced in another document as a URL to a SMART EC website. The text itself may not be published commercially in print or electronic form, edited, translated, or otherwise altered without the permission of SMART EC.

It is possible that this publication may contain reference to or information about SMART EC products, programming, or services that are not available in your country. Such references or information must not be construed to mean that SMART EC intends to announce such SMART EC products, programming, or services in your country.

Limited and Restricted Rights Legend

If the documentation contained herein is supplied, directly or indirectly, to the U.S. Government, the following notice shall apply unless otherwise agreed to in writing by SMART Embedded Computing.

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data clause at DFARS 252.227-7013 (Nov. 1995) and of the Rights in Noncommercial Computer Software and Documentation clause at DFARS 252.227-7014 (Jun. 1995).

SMART Embedded Computing™, Inc.

2900 S. Diablo Way, Suite 190

Tempe, Arizona 85282

USA

*For full legal terms and conditions, visit *www.smartembedded.com/ec/legal*

Table of Contents

Table of Contents

List of Figures

List of Figures

List of Tables

List of Tables

About this Manual

Overview of Contents

Network administrators and application developers intending to configure SRstackware® Layer 2 protocols should use this Configuration Guide.

This guide attempts to make configuration simpler by adding topology illustrations and configuration samples. It covers basic configurations for SRstackware Layer 2 protocols, including STP, RSTP, MSTP, VLAN, LACP, GMRP, and GVRP IGMP Snooping. Use this guide together with the *Layer 2 Command Reference, Layer 3 Command Reference,* and the *Switch Configuration Command Reference* to get complete information on the commands used in the configurations displayed in this guide.

The configurations in this guide are for the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, refer to the *SRstackware Hybrid Developer Guide*.

This manual is divided into the following chapters and appendix.

Abbreviations

This document uses the following abbreviations:

Abbreviation	Definition
ACE	Access Control Entry
ACL	Access Control List
CoS	Class of Service
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
IGMP	Internet Group Management Protocol
LACP	Link Aggregation Control Protocol
MSTP	Multiple Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol
STP	Spanning Tree Protocol
QoS	Quality of Service
WRR	Weighted Round Robin

Conventions

The following table describes the conventions used throughout this manual.

Notation	Description
0x00000000	Typical notation for hexadecimal numbers (digits are 0 through F), for example used for addresses and offsets
0b0000	Same for binary numbers (digits are 0 and 1)
bold	Used to emphasize a word
`Screen`	Used for on-screen output and code related elements or commands. `Sample of Programming used in a table (9pt)`
`Courier + Bold`	Used to characterize user input and to separate it from system output
Reference	Used for references and for table and figure descriptions
File > Exit	Notation for selecting a submenu

Notation	Description
<text>	Notation for variables and keys
[text]	Notation for software buttons to click on the screen and parameter description
...	Repeated item for example node 1, node 2, ..., node 12
. . .	Omission of information from example/command that is not necessary at the time
..	Ranges, for example: 0..4 means one of the integers 0,1,2,3, and 4 (used in registers)
|	Logical OR
	Indicates a hazardous situation which, if not avoided, could result in death or serious injury
	Indicates a hazardous situation which, if not avoided, may result in minor or moderate injury
	Indicates a property damage message
	Indicates a hot surface that could result in moderate or serious injury
	Indicates an electrical situation that could result in moderate injury or death
	Indicates that when working in an ESD environment care should be taken to use proper ESD practices

Notation	Description
	No danger encountered, pay attention to important information

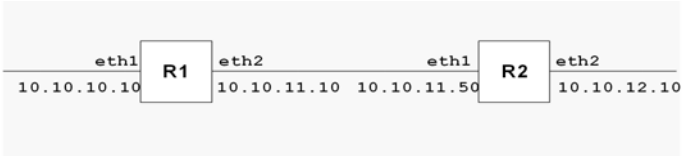
Summary of Changes

This manual has been revised and replaces all prior editions.

Part Number	Publication Date	Description
6806800N86E	March 2020	Rebranded to SMART Embedded Computing. Light editing and formatting. Updated Abbreviations table.
6806800N86D	July 2017	Added registered trademark to SRstackware.
6806800N86C	June 2014	Rebranded to Artesyn template.
6806800N86B	October 2012	Added a note in*Chapter 7, IGMP Snooping Configuration* that the sections are relevant only if LAYER3SRS is licensed.
6806800N86A	February 2012	EA Release

Introduction

1.1 Format Used in the Configuration Examples

Format	Description
Scenario Description The examples begin with a description of the topology and the scenario. This is an explanation of what is to be achieved by the specified configuration.	Enabling RIP This example shows the minimum configuration required for enabling RIP on an interface.....
Illustration This section includes the illustration of the complete topology used in the example. The figure uses the exact IP addresses and names of routers used in the example.	
Configuration Includes the complete configuration of the routers involved in the example. The prompt shows the execution modes of the commands. Each example begins from the Privileged Exec mode. The method to reach every command mode is illustrated in the *Daemon Command Modes* section. For modes specific to different protocols, please refer to the corresponding Command Reference (for OSPF command modes, refer to the *OSPF Command Reference*). Explanation This is the grey section next to the configuration statements and is not to be typed in the CLI. It provides step-by-step explanation of the actions performed by the configuration.	R1 # configure terminal (config)# router rip (config-router)# net.. `(config-router)# net..` Enter the Configure mode. Define the RIP process... Associate networks with....

Format	Description
Names of Commands Used This section lists the names of the commands used in the example. Use these command names to look up the command details in the Command References. To avoid repetition, this list does not include a few common commands such as `configure terminal` or `interface`. These common commands are explained in the *Switch Configuration Command Reference*.	Names of Commands Used router rip, network
Validation Commands These commands are usually show commands that display outputs and are used to validate the configuration.	Validation Commands show ip rip

1.2 Command Line Interface Primer

The SRstackware® Command Line Interface (CLI) is a text-based facility similar to industry standards. Many of the commands may be used in scripts to automate many configuration tasks. Each CLI command is usually associated with a specific function or a common function performing a specific task. Multiple users can telnet and issue commands using the Exec mode and the Privileged Exec mode. However, only one user is allowed to use the Configure mode at a time, to avoid multiple users from issuing configuration commands simultaneously.

The VTY shell, described in the *SRstackware VTY Shell User Guide*, gives users and administrators the ability to issue commands to several daemons from a single telnet session.

1.2.1 Command Line Help

The SRstackware CLI contains a text-based help facility. Access this help by typing in the full or partial command string then typing: ?. The SRstackware CLI displays the command keywords or parameters plus a short description.

For example, at the CLI command prompt, type `show ?` (the CLI does not display the question mark).

The CLI displays this keyword list with short descriptions for each keyword:

```
bgpd# show
  debugging       Debugging functions (see also 'undebug')
  history         Display the session command history
  ip              IP information
  memory          Memory statistics
  route-map       route-map information
  running-config  running configuration
  startup-config  Contents of startup configuration
  version         Displays SRstackware version
```

1.2.2 Syntax Help

The SRstackware CLI can complete the spelling of command or parameter keywords. Begin typing the command or parameter then press TAB. At the CLI command prompt type `sh:`

```
Router> sh
```

Press TAB. The CLI shows:

```
Router> show
```

If the command or parameter partial spelling is ambiguous, the SRstackware CLI displays the choices that match the abbreviation. Type `show i`. Press TAB. The CLI shows:

```
Router> show i
interface  ip
Router> show i
```

The interface displays the `interface` and `ip` keywords. Type n to select `interface` and press TAB. The CLI shows:

```
Router> show in
Router> show interface
```

Type `?` and the CLI shows the list of parameters for the `show interface` command.

```
  [IFNAME]  Interface name
Router> show interface
```

This command has but one positional parameter, an interface name. Supply a value for the `IFNAME` parameter.

1.2.2.1 Command Abbreviations

The SRstackware CLI accepts abbreviations for commands. For example,

```
sh in 7
```

is the abbreviation for the show `interface` command.

1.2.2.2 Command Line Errors

If the router does not recognize the command after ENTER is pressed, it displays this message:

```
%  Invalid input detected at '^' marker.
```

If a command is incomplete it displays this message:

```
% Incomplete command.
```

Some commands are too long for the display line and can wrap in mid-parameter or mid-keyword if necessary:

```
area 10.10.0.18 virtual-link 10.10.0.19 authentication-key 57393
```

1.3 Daemon Command Modes

The commands available for each protocol are separated into several modes (nodes) arranged in a hierarchy, Exec is the lowest. Each mode has its own special commands, in some modes, commands from a lower mode are available.

Multiple users can telnet and issue commands using the Exec mode and the Privileged Exec mode. However, only one user is allowed to use the Configure mode at a time, to avoid multiple users from issuing configuration commands simultaneously.

1.3.1 Modes Common to Protocols

Exec

This mode, also called the View mode, is the base mode from where users can perform basic commands like show, exit, quit, help, list, and enable. All SRstackware daemons have this mode.

Privileged Exec

This mode, also called the Enable mode, allows users to perform debugging commands, the write commands (for saving and viewing the configuration), show commands, and so on.

Configure

Sometimes referred to as Configure Terminal, this mode serves as a gateway into the Interface, Router, Line, Route Map, Key Chain and Address Family modes. All SRstackware daemons have this mode.

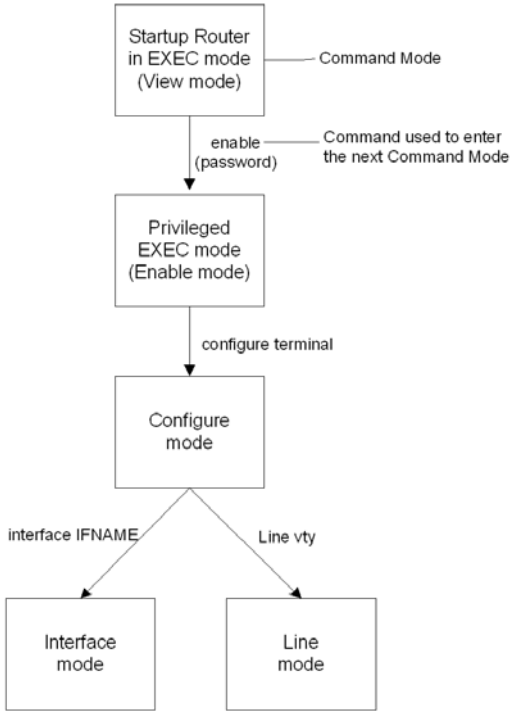
Interface

This mode is used to configure protocol-specific settings for a particular interface. Any attribute configured in this mode overrides an attribute configured in the router mode.

Line

This mode makes available access-class commands.

Figure 1-1 Modes Common to Protocols



1.3.2 Modes Specific to Protocols

The following command modes are not common to all protocols and the command used to enter these modes is different for different protocols. For an illustration of these command modes refer to the corresponding *Command Reference* documents.

Router

Sometimes referred to as Configure Router mode, this mode is available for the LDP, BGP, OSPF, RSVP-TE and RIP protocols only and makes available router and routing commands.

Route-map

This mode is used to set route metric, route-length and cost data. It is available for the BGP, OSPF, and RIP protocols only.

Address Family

This mode allows support for multiprotocol BGP extension. It includes address family-specific commands.

Key Chain

This mode, available for the RIP protocol only, manages the key chain.

Trunk

This mode is used to create or modify RSVP trunks. A trunk is the static definition for a Labeled Switch Path (LSP). Each trunk creates a corresponding LSP, and this LSP is signaled from the machine where the trunk was created, to the egress, as specified in the trunk's configuration.

Path

Use this mode to create or modify RSVP paths. You can define a possible path to be taken between two points in a network. This path could be a complete description (with each node specified) or a partial one specifying certain hops that the path must take.

STP Configuration

2.1 Introduction

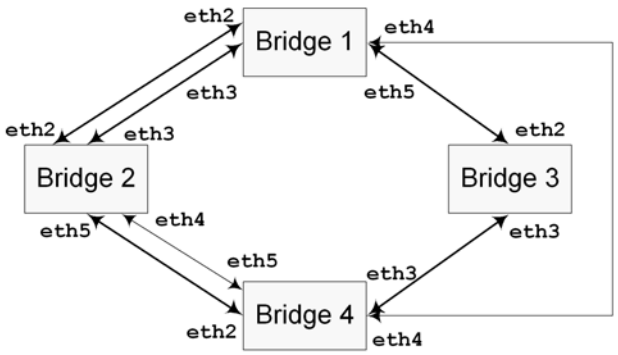
This chapter contains a complete sample STP configuration. To see details on the commands used in this example refer to the SRstackware® *Layer 2 Command Reference*. To avoid repetition, some common commands, like `configure terminal`, have not been listed under the *Commands Used* section. The *Switch Configuration Command Reference* explains these common commands.

2.2 Configuring STP

STP prevents duplication of packets by eliminating loops in the network. This example gives a simple multi-bridge topology and how to configure it

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

Figure 2-1 STP Configuration



Bridge 1	
# configure terminal	Enter the Configure mode.
(config)# bridge 1 protocol ieee	Add a bridge (1) to the spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.

Bridge 1	
(config-if)# bridge-group 1	Associate the interface eth2 with bridge group 1.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth3 with bridge group 1.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth4 with bridge group 1.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth5 with bridge group 1.

Bridge 2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol ieee	Add a bridge (2) to the spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 2`	Associate the interface eth2 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth3 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth4 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

Bridge 2	
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth5 with bridge group 2.

Bridge 4	
# configure terminal	Enter the Configure mode.
(config)# bridge 4 protocol ieee	Add a bridge (4) to the spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 4`	Associate the interface eth2 with bridge group 4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth3 with bridge group 4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth4 with bridge group 4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth5 with bridge group 4.

Bridge 3	
# configure terminal	Enter the Configure mode.
(config)# bridge 3 protocol ieee	Add a bridge (3) to the spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 3`	Associate the interface eth2 with bridge group 3.

Bridge 3	
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 3	Associate the interface eth3 with bridge group 3.

Names of Commands Used

`bridge protocol ieee, bridge-group`

Validation Commands

`show spanning-tree, show bridge`

For sample outputs of the validation commands, refer to *STP Configuration on page 81*.

RSTP Configuration

3.1 Introduction

This chapter contains a complete sample Rapid Spanning Tree Protocol (RSTP) configuration. To see details on the commands used in this example, refer to the SRstackware® *Layer 2 Command Reference*. To avoid repetition, some common commands, like `configure terminal`, have not been listed under the *Commands Used* section. The *Switch Configuration Command Reference* explains these common commands.

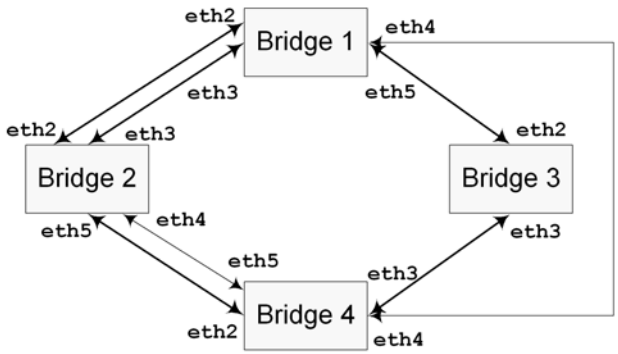
3.2 Configuring RSTP

The RSTP provides rapid convergence of the spanning tree. It speeds up the reconfiguration of the tree after a change by having alternate ports.

This example gives a simple multi-bridge topology and how to configure it.

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

Figure 3-1 RSTP Configuration



Bridge 1	
# configure terminal	Enter the Configure mode.
(config)# bridge 1 protocol rstp	Add a bridge (1) to the rapid spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth2 with bridge group 1.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth3 with bridge group 1.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth4 with bridge group 1.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth5 with bridge group 1.

Bridge 2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol rstp	Add a bridge (2) to the rapid spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth2 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth3 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

Bridge 2	
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth4 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth5 with bridge group 2.

Bridge 3	
# configure terminal	Enter the Configure mode.
(config)# bridge 3 protocol rstp	Add a bridge (3) to the rapid spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
(config-if)# bridge-group 3	Associate the interface eth2 with bridge group 3.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 3	Associate the interface eth3 with bridge group 3.

Bridge 4	
# configure terminal	Enter the Configure mode.
(config)# bridge 4 protocol rstp	Add a bridge (4) to the rapid spanning tree table
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth2 with bridge group 4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth3 with bridge group 4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

Bridge 4	
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth4 with bridge group 4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth5 with bridge group 4.

Names of Commands Used

`bridge protocol rstp, bridge-group`

Validation Commands

`show spanning-tree, show bridge`

For sample outputs of the validation commands, refer to *RSTP Configuration on page 82*.

MSTP Configuration

4.1 Introduction

This chapter contains a complete sample Multiple Spanning Tree Protocol (MSTP) configuration. To see details on the commands used in this example, refer to the SRstackware® *Layer 2 Command Reference*. To avoid repetition, some common commands, like `configure terminal`, have not been listed under the *Commands Used* section. The *Switch Configuration Command Reference* explains these common commands.

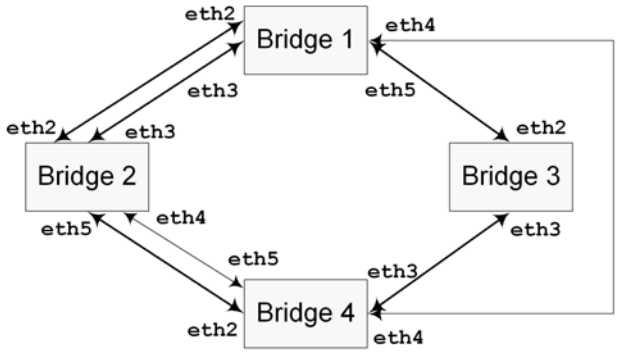
4.2 Configuring MSTP

MSTP allows multiple VLANs to be grouped into one spanning-tree instance. Every MST instance has a spanning-tree which is independent of other spanning-tree instances providing multiple forwarding paths for data traffic.

This example gives a simple multi-bridge topology and its configuration.

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

Figure 4-1 MSTP Configuration



Bridge 1	
# configure terminal	Enter the Configure mode.
(config)# bridge 1 protocol mstp	Add a bridge (1) to the multiple spanning tree table.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 2 bridge 1 state enable	Enable the state of VLAN 2 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 1.
(config-vlan)# vlan 3 bridge 1 state enable	Enable the state of VLAN 3 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 1.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree Configuration mode.
(config-mst)# bridge 1 instance 2 vlan 2	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# bridge 1 instance 3 vlan 3	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
(config)# interface eth2	Enter the Interface mode for eth2
(config-if)# bridge-group 1 instance 2 priority 50	Assign bridge-group 1 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Enter the Interface mode for eth3.

Bridge 1	
(config-if)# bridge-group 1 instance 3 priority 55	Assign bridge-group 1 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
(config)# interface eth4	Enter the Interface mode for eth4.
(config-if)# bridge-group 1 instance 4 priority 50	Assign bridge-group 1 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Enter the Interface mode for eth5.
(config-if)# bridge-group 1 instance 5 priority 55	Assign bridge-group 1 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.

Bridge 2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol mstp	Add a bridge (2) to the multiple spanning tree table.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 2 bridge 2 state enable	Enable the state of VLAN 2 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 2.
(config-vlan)# vlan 3 bridge 2 state enable	Enable the state of VLAN 3 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 2.

Bridge 2	
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree Configuration mode.
(config-mst)# bridge 2 instance 2 vlan 2	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# bridge 2 instance 3 vlan 3	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
`(config)# interface eth2`	Enter the Interface mode for eth2.
(config-if)# bridge-group 2 instance 2 priority 50	Assign bridge-group 2 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
`(config)# interface eth3`	Enter the Interface mode for eth3.
(config-if)# bridge-group 2 instance 3 priority 55	Assign bridge-group 2 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
`(config)# interface eth4`	Enter the Interface mode for eth4.

Bridge 2	
(config-if)# bridge-group 2 instance 4 priority 50	Assign bridge-group 2 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
`(config)# interface eth5`	Enter the Interface mode for eth5.
(config-if)# bridge-group 2 instance 5 priority 55	Assign bridge-group 2 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.

Bridge 3	
# configure terminal	Enter the Configure mode.
(config)# bridge 3 protocol mstp	Add a bridge (3) to the multiple spanning tree table.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 2 bridge 3 state enable	Enable the state of VLAN 2 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 3.
(config-vlan)# vlan 3 bridge 3 state enable	Enable the state of VLAN 3 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 3.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree Configuration mode.
(config-mst)# bridge 3 instance 2 vlan 2	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.

Bridge 3	
(config-mst)# bridge 3 instance 3 vlan 3	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
`(config)# interface eth2`	Enter the Interface mode for eth2
(config-if)# bridge-group 3 instance 2 priority 50	Assign bridge-group 3 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
`(config)# interface eth3`	Enter the Interface mode for eth3.
(config-if)# bridge-group 3 instance 3 priority 55	Assign bridge-group 3 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.

Bridge 4	
# configure terminal	Enter the Configure mode.
(config)# bridge 4 protocol mstp	Add a bridge (4) to the multiple spanning tree table.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 2 bridge 4 state enable	Enable the state of VLAN 2 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 4.
(config-vlan)# vlan 3 bridge 4 state enable	Enable the state of VLAN 3 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 4.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.

Bridge 4	
(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree Configuration mode.
(config-mst)# bridge 4 instance 2 vlan 2	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# bridge 4 instance 3 vlan 3	Create an instance of VLAN.The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
`(config)# interface eth2`	Enter the Interface mode for eth2
`(config-if)# bridge-group 4 instance 2 priority 50`	Assign bridge-group 4 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
`(config)# interface eth3`	Enter the Interface mode for eth3.
(config-if)# bridge-group 4 instance 3 priority 55	Assign bridge-group 4 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
(config-mst)# exit	Exit MST Configuration mode and enter the Configure mode.
`(config)# interface eth4`	Enter the Interface mode for eth4.
(config-if)# bridge-group 4 instance 4 priority 50	Assign bridge-group 4 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.

Bridge 4	
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
`(config)# interface eth5`	Enter the Interface mode for eth5.
(config-if)# bridge-group 4 instance 5 priority 55	Assign bridge-group 4 to this instance and set a port priority for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.

Names of Commands Used

`bridge protocol mstp, bridge instance priority, bridge-group instance priority, spanning tree mst, vlan bridge`

Validation Commands

`show spanning-tree mst detail, show bridge, show spanning-tree mst instance`

For sample outputs of the validation commands, refer *MSTP Configuration on page 83*.

VLAN Configuration

5.1 Introduction

This chapter contains a complete sample VLAN configuration. To see details on the commands used in this example, or to see the outputs of the validation commands, refer to the SRstackware® *Layer 2 Command Reference*. To avoid repetition, some common commands, like `configure terminal`, have not been listed under the *Commands Used* section. The *Switch Configuration Command Reference* explains these common commands.

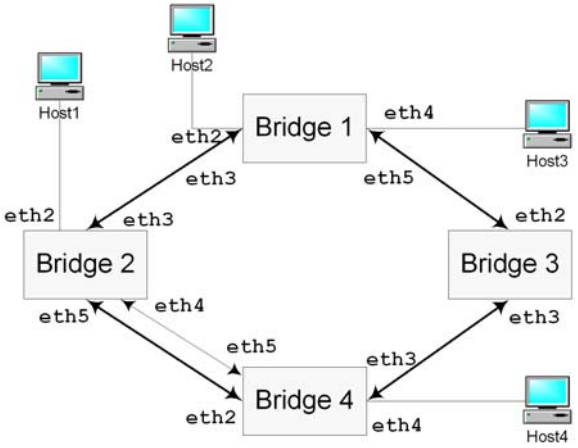
5.2 Configuring VLAN

This sample shows configuration of a spanning tree bridge with VLAN tags on forwarding frames. VLAN port access is configured on port `eth2` on bridge 2, port `eth2` and `eth4` on bridge 1 and port `eth4` on bridge 4. Incoming tagged packets to bridge 2 will be forwarded only on these ports configured with VLAN port access.

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

To enable routing through VLANs, use the intervlan-route enable option, while creating the VLAN.

Figure 5-1 VLAN Configuration



Bridge 1	
# configure terminal	Enter the Configure mode.
(config)# bridge 1 protocol ieee vlan-bridge	Specify VLAN for bridge 1.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 5 bridge 1 state enable	Enable VLAN (5) on bridge 1. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 1`	Associate the interface eth2 with bridge group 1.
(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)# switchport access vlan 5	Enable VLAN port access by specifying the VLAN ID 5 on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth3 with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth4 with bridge group 1.
(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode.

Bridge 1	
(config-if)# switchport access vlan 5	Enable VLAN port access by specifying the VLAN ID 5 on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 1	Associate the interface eth5 with bridge group 1.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.

Bridge 2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol ieee vlan-bridge	Specify VLAN for bridge 2.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 5 bridge 2 state enable	Enable VLAN (5) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 2`	Associate the interface eth2 with bridge group 2.
(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)# switchport access vlan 5	Enable VLAN port access by specifying the VLAN ID 5 on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth3 with bridge group 2.

Bridge 2	
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth4 with bridge group 2.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth5 with bridge group 2.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.

Bridge 4	
# configure terminal	Enter the Configure mode.
(config)# bridge 4 protocol ieee vlan-bridge	Specify VLAN for bridge 4.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 5 bridge 4 state enable	Enable VLAN (5) on bridge 4. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.

Bridge 4	
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 4`	Associate the interface eth2 with bridge group 4.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth3 with bridge group 4.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth4	Specify the interface (eth4)to be configured and enter the Interface mode.
`(config-if)# bridge-group 4`	Associate the interface eth4 with bridge group 4.
(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)# switchport access vlan 5	Enable VLAN port access by specifying the VLAN ID 5 on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth5	Specify the interface (eth5)to be configured and enter the Interface mode.
(config-if)# bridge-group 4	Associate the interface eth5 with bridge group 4.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.

Bridge 4	
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.

Bridge 3	
# configure terminal	Enter the Configure mode.
(config)# bridge 3 protocol ieee vlan-bridge	Specify VLAN for bridge 3.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 5 bridge 3 state enable	Enable VLAN (4) on bridge 3. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 3`	Associate the interface eth2 with bridge group 3.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 3	Associate the interface eth3 with bridge group 3.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
`(config-if)# switchport trunk allowed vlan all`	Enable all VLAN IDs on this port.

Names of Commands Used

```
bridge protocol ieee vlan-bridge, bridge-group, vlan bridge
```

Validation Commands

```
show spanning-tree, show bridge, show vlan all bridge
```

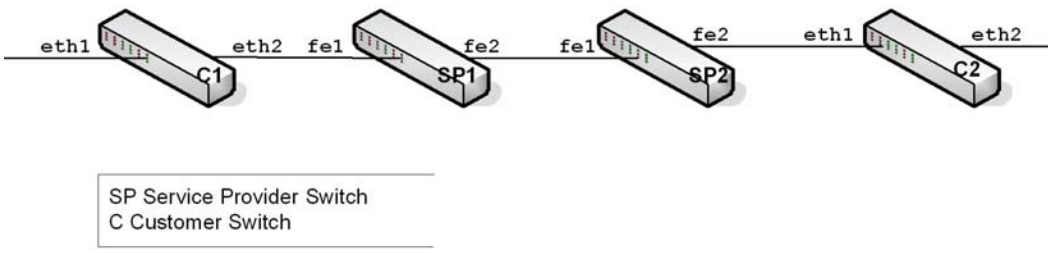
5.3 Configuring VLAN Stacking

The SRstackware VLAN Stacking implementation offers multiple virtual LANs over a single circuit. It assigns two VLAN IDs to each frame header.

In this configuration example, two customer switches, C1 and C2 are connected to each other using two Service Provider switches, SP1 and SP2. VLAN stacking is enabled on interface fe1 of switch SP1 and interface fe2 of switch SP2. This allows tagged traffic of Customer Switches C1 and C2 through the edge ports of the Service Provider Switches SP1 and SP2.

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

Figure 5-2 VLAN Stacking



At SP1	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol ieee vlan-bridge	Specify VLAN for bridge 2.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 2 bridge 2 state enable	Enable VLAN (2) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# interface fe1	Specify the interface (fe1)to be configured and enter the Interface mode.
(config-if)# no shutdown	Bring the bridge instance into operation with the no shutdown command.
`(config-if)# bridge-group 2`	Associate the interface fe1 with bridge group 2.
(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)# switchport vlan-stacking customer-edge-port	Enable VLAN stacking on this interface.
(config-if)# switchport access vlan 2	Enable VLAN port access by specifying the VLAN ID 2 on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface fe2	Specify the interface (fe2)to be configured and enter the Interface mode.
(config-if)# no shutdown	Bring the bridge instance into operation with the no shutdown command.
`(config-if)# bridge-group 2`	Associate the interface fe1 with bridge group 2.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 2	Enable VLAN ID 2 on this port.
(config-if)# switchport vlan-stacking provider-port	Enable VLAN stacking on this interface.

At SP1	
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

At SP2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol ieee vlan-bridge	Specify VLAN for bridge 2.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 2 bridge 2 state enable	Enable VLAN (2) on bridge 2. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# interface fe2	Specify the interface (fe2)to be configured and enter the Interface mode.
(config-if)# no shutdown	Bring the bridge instance into operation with the no shutdown command.
`(config-if)# bridge-group 2`	Associate the interface fe1 with bridge group 2.
(config-if)# switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)# switchport vlan-stacking customer-edge-port	Enable VLAN stacking on this interface.
(config-if)# switchport access vlan 2	Enable VLAN port access by specifying the VLAN ID 2 on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface fe1	Specify the interface (fe1)to be configured and enter the Interface mode.
(config-if)# no shutdown	Bring the bridge instance into operation with the no shutdown command.
`(config-if)# bridge-group 2`	Associate the interface fe1 with bridge group 2.
(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)# switchport trunk allowed vlan add 2	Enable VLAN ID 2 on this port.

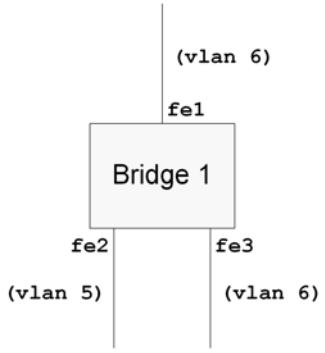
At SP2	
(config-if)# switchport vlan-stacking provider-port	Enable VLAN stacking on this interface.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

5.4 Configuring VLAN Classifiers

SRstackware offers the ability to use VLAN classifiers to define specific rules for directing packets to selected VLANs based on protocol or subnet criteria. Sets of rules can be grouped (one group per interface).

In this configuration example, two VLAN classifier rules are created to direct IPv6 packets and packets sourced from subnet 1.1.1.1/24 to VLAN 5 from interface (fe1) on bridge 1. Packets that do not meet the criteria defined by the rules are passed by default to VLAN 6.

Figure 5-3 Configuring VLAN Classifiers



Configuring VLAN Classifiers	
# configure terminal	Enter the Configure mode.
(config)# bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 6 bridge 1	Enable VLAN 6 on bridge 1.
(config-vlan)# vlan 5 bridge 1	Enable VLAN 5 on bridge 1.

Configuring VLAN Classifiers	
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# vlan classifier rule 1 ipv4 1.1.1.1/24 vlan 5	Create a subnet-based VLAN classifier rule (sources from subnet 1.1.1.1/24 are sent to VLAN 5).
(config)# vlan classifier rule 2 proto ipv6 encap ethv2 vlan 5	Create a protocol-based VLAN classifier rule (IPv6 packets with Ethernet encapsulation are sent to VLAN 5).
(config)# vlan classifier group 1 add rule 1	Create a group of rules (add rule 1 to group 1).
(config)# vlan classifier group 1 add rule 2	Add rule 2 to group 1.
(config)# interface fe1	Enter the Interface mode.
(config-if)# switchport	Switch to Layer 2 mode (if you were using the Exit the Interface mode and enter the Configure mode. Hybrid Layer 2/Layer 3 module).
(config-if)# bridge group 1	Associate interface fe1 to bridge 1.
(config-if)# switchport access vlan 6	Assign PVID 6 to port fe1.
(config-if)# vlan classifier activate 1	Activate group 1 on interface fe1. Packets matching the group will be switched to VLAN 5.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

Names of Commands Used

```
vlan bridge, vlan classifier rule, vlan classifier group rule,
switchport access vlan, vlan classifier activate
```

Validation Commands

```
show vlan classifier group, show vlan classifier rule
```

For sample outputs of the validation commands, refer to *VLAN Configuration on page 96*.

LACP Configuration

6.1 Introduction

This chapter contains a complete sample Link Aggregation Control Protocol (LACP) configuration. To see details on the commands used in this example, or to see the outputs of the validation commands, refer to the SRstackware® *Layer 2 Command Reference*. To avoid repetition, some common commands, like `configure terminal`, have not been listed under the *Commands Used* section. The *Switch Configuration Command Reference* explains these common commands.

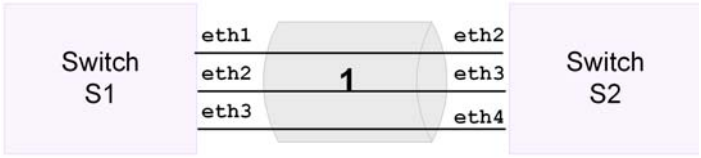
LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as 2 or 3 interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption.

The SRstackware LACP implementation supports the aggregation of maximum eight physical Ethernet links into a single logical channel.

6.2 Configuring LACP

In this example, three links are configured between the two switches S1 and S2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by the STP as one interface.

Figure 6-1 LACP Configuration



S1	
# configure terminal	Enter the Configure mode.
(config)# lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
(config)# interface eth1	Enter the Interface mode and configure this interfaces properties.
(config-if)# channel-group 10 mode active	Add this interface to a channel group 10 and enable link aggregation so that it may be selected for aggregation by the local system.
(config-if)# exit	Exit the Interface mode and enter Configure mode.
(config)# interface eth2	Enter the Interface mode and configure this interfaces properties.
(config-if)# channel-group 10 mode active	Add this interface to a channel group 10 and enable link aggregation so that it may be selected for aggregation by the local system.
(config-if)# exit	Exit the Interface mode and enter Configure mode.
(config)# interface eth3	Enter the Interface mode and configure this interfaces properties.
(config-if)# channel-group 10 mode active	Add this interface to a channel group 10 and enable link aggregation so that it may be selected for aggregation by the local system.

S2	
# configure terminal	Enter the Configure mode.
(config)# lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
(config)# interface eth2	Enter the Interface mode and configure this interfaces properties.
(config-if)# channel-group 10 mode active	Add this interface to a channel group 10 and enable link aggregation so that it may be selected for aggregation by the local system.

S2	
(config-if)# exit	Exit the Interface mode and enter Configure mode.
(config)# interface eth3	Enter the Interface mode and configure this interfaces properties.
(config-if)# channel-group 10 mode active	Add this interface to a channel group 10 and enable link aggregation so that it may be selected for aggregation by the local system.
(config-if)# exit	Exit the Interface mode and enter Configure mode.
(config)# interface eth4	Enter the Interface mode and configure this interfaces properties.
(config-if)# channel-group 10 mode active	Add this interface to a channel group 10 and enable link aggregation so that it may be selected for aggregation by the local system.

Names of Commands Used

`lacp system-priority, channel-group mode`

Validation Commands

`show lacp sys-id, show port etherchannel po10, show etherchannel summary, show etherchannel`

For sample outputs of the validation commands, refer to *LACP Configuration on page 97*.

6.3 Configuring Load Balancing in LACP

In this example, we assume that the sample configuration provided in the *Configuring LACP on page 49* section is already completed. We need to configure the load balancing algorithm to be used on the aggregator interface as follows.

S1	
# configure terminal	Enter the `Configure` mode.
(config)# interface po10	Enter the `Interface` mode and configure this Aggregator interfaces properties.
(config-if)# port-channel load-balance src-mac	Configure the load balancing algorithm to src-mac. The traffic flowing through the aggregator interface will be load balanced based on the source mac address.

(config-if)# exit	Exit the `Interface` mode and enter `Configure` mode.

S2	
# configure terminal	Enter the `Configure` mode.
(config)# interface po10	Enter the `Interface` mode and configure this Aggregator interfaces properties.
(config-if)# port-channel load-balance src-mac	Configure the load balancing algorithm to src-mac. The traffic flowing through the aggregator interface will be load balanced based on the source mac address.
(config-if)# exit	Exit the `Interface` mode and enter `Configure` mode.

Names of Commands Used

`port-channel load-balance`

Validation Commands

`show port etherchannel, show etherchannel detail`

IGMP Snooping Configuration

7.1 Introduction

This chapter provides steps to configure Internet Group Management Protocol (IGMP) Snooping. To see details on the commands used in this example, or to see the outputs of the validation commands, refer to the SRstackware® *Layer 2 Command Reference*. To avoid repetition, some common commands, such as, `configure terminal`, have not been listed under the *Commands Used* section. The *SRstackware® Intelligent Network Software Switch Configuration Command Reference* explains these common commands.

This chapter is relevant, only if LAYER3SRS is licensed.

This configuration sample assumes that you are running the SRstackware Layer 2 module. If using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

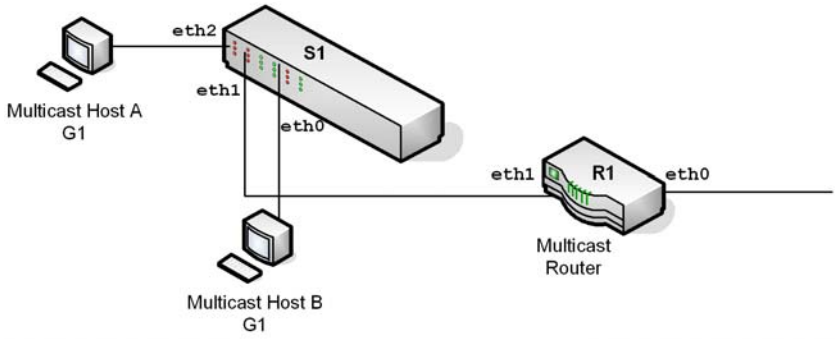
Without IGMP, Layer 2 switches handle IP multicast traffic in the same manner as broadcast traffic, and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Only one membership report is relayed from a group, instead of a report from each host in the group. To achieve this, IGMP proxy is enabled on the switches.

This example describes the configuration on switch S1. The interface, eth1, is configured as a multicast router port. Because IGMP Snooping is used in bridged LAN environments only, router R1 does not require running IGMP Snooping, and can run any multicast protocol (such as PIM-SM). Thus, the configuration on R1 is not included in this example.

To enable IGMP Snooping on an interface:

- Add a bridge to the spanning-tree table.
- Specify the interface to be configured.
- Associate the interface with bridge group.
- Enable IGMP Snooping globally.
- Enable IGMP Snooping on the bridge group.
- Configure ports that are connected to routers as multicast router ports.
- By default, IGMP report suppression is enabled on the switch

Figure 7-1 IGMP Snooping Configuration



As a result of this configuration:

- The switch, itself will reply back with Membership report messages in response to queries received on interface eth1. However, if you do not enable report suppression on the switch when it receives an IGMP Query message on eth1, it forwards it to both Host A and Host B. As a result, both hosts reply with a Membership report (as Layer 2 IGMP is running on the hosts).
- Because Host A and Host B are members of the same multicast group, the router is not notified when Host A leaves the group, because the group still has another member Host B remaining. When Host B also leaves the group, the switch will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

You can verify the above configuration by running ethereal and tethereal on the interfaces of the switch and hosts

Switch S1	
# configure terminal	Enter the Configure mode.
(config)# bridge 1 protocol ieee vlan-bridge	Add bridge 1 to the spanning-tree table.
(config)# interface eth0	Specify the interface eth0 to be configured, and enter the Interface mode.
(config-if)# shutdown	Shut down the interface.
(config-if)# switchport	Configure the interface as a switch port.
(config-if)# bridge-group 1	Associate the interface eth1 with bridge-group 1.
(config-if)# switchport mode access	Configure the port as an access port.
(config-if)# no shutdown	Bring up the interface.
(config-if)# exit	Exit the Interface mode, and enter the Configure mode.
(config)# interface eth1	Specify interface eth1 to be configured, and enter the Interface mode.
(config-if)# shutdown	Shut down the interface.
(config-if)# switchport	Configure the interface as a switch port.
(config-if)# bridge-group 1	Associate interface eth1 with bridge-group 1.
(config-if)# switchport mode access	Configure the port as an access port.
(config-if)# no shutdown	Bring up the interface.
(config-if)# exit	Exit the Interface mode, and enter the Configure mode.
(config)# interface eth2	Specify interface eth2 to be configured, and enter the Interface mode.
(config-if)# shutdown	Shut down the interface.
(config-if)# switchport	Configure the interface as a switch port.
(config-if)# bridge-group 1	Associate interface eth2 with bridge-group 1.
(config-if)# switchport mode access	Configure the port as an access port.
(config-if)# no shutdown	Bring up the interface.
(config-if)# exit	Exit the Interface mode, and enter the Configure mode.

Switch S1	
(config)# ip igmp snooping	Enable IGMP Snooping globally.
(config)# interface vlan1.1	Specify interface vlan1.1 to be configured, and enter the Interface mode.
(config-if)# ip igmp snooping mrouter interface eth1	Configure this port as a multicast router port.

Names of Commands Used

```
ip igmp snooping, switchport mode access, switchport, bridge
protocol ieee, bridge-group, ip igmp snooping mrouter
```

Validation Commands

```
show bridge, show ip igmp interface vlan1.1, show ip igmp groups
```

For sample outputs of the validation commands, refer to *IGMP Snooping Configuration on page 98*.

GMRP Configuration

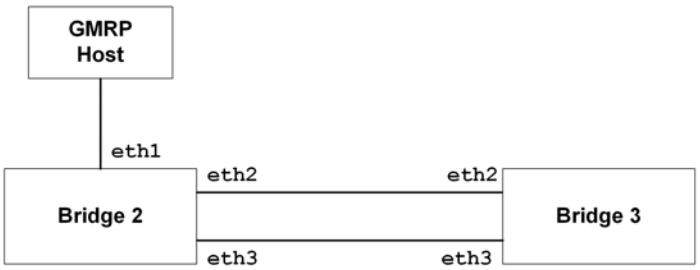
8.1 Configuring GMRP

GARP Multicast Registration Protocol (GMRP) allows bridges and hosts to register group membership information with the MAC bridges on the network.

In this example, bridge 2 is forwarding multicast packets coming from the Host to the gmrp-enabled bridge 3. To configure GMRP on a bridge, enable spanning tree on the bridge, disable IGMP snooping, and associate interfaces with the bridge group. Then enable GMRP on all ports for the bridge.

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

Figure 8-1 GMRP Configuration



Bridge 2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol ieee vlan-bridge	Add a bridge (2) to the spanning tree table
(config)# bridge 2 spanning-tree enable	Enable the Spanning Tree Protocol commands on this bridge.
(config)# no ip igmp snooping	Globally disable IGMP snooping.
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 2`	Associate the interface eth2 with bridge group 2.

Bridge 2	
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth3 with bridge group 2.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# set gmrp enable bridge 2	Enable GMRP on all ports for bridge 2.
(config)# set port gmrp enable eth2	Enable GMRP on port eth2.
(config)# set gmrp fwdall enable eth2	Enable GMRP forwarding on port eth2.
(config)# set port gmrp enable eth3	Enable GMRP on port eth3.
(config)# set gmrp fwdall enable eth3	Enable GMRP forwarding on port eth3.

Bridge 3	
# configure terminal	Enter the Configure mode.
(config)# bridge 3 protocol ieee vlan-bridge	Add a bridge (3) to the spanning tree table.
(config)# bridge 3 spanning-tree enable	Enable the Spanning Tree Protocol commands on this bridge.
(config)# no ip igmp snooping	Globally disable IGMP snooping.
(config)# interface eth2	Specify the interface (eth2)to be configured and enter the Interface mode.
`(config-if)# bridge-group 3`	Associate the interface eth2 with bridge group 3.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# interface eth3	Specify the interface (eth3)to be configured and enter the Interface mode.
(config-if)# bridge-group 3	Associate the interface eth3 with bridge group 3.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# set gmrp enable bridge 3	Enable GMRP on all ports for bridge 3.

Bridge 3	
(config)# set port gmrp enable eth2	Enable GMRP on port eth2.
(config)# set gmrp fwdall enable eth2	Enable GMRP forwarding on port eth2.
(config)# set port gmrp enable eth3	Enable GMRP on port eth3.
(config)# set gmrp fwdall enable eth3	Enable GMRP forwarding on port eth3.

Names of Commands Used

`ip igmp snooping, set gmrp, bridge spanning-tree enable, bridge protocol ieee, set port gmrp, set gmrp fwdall`

Validation Commands

`show gmrp configuration, show gmrp timer`

For sample outputs of the validation commands, refer to *GMRP Configuration on page 99*.

GVRP Configuration

9.1 Configuring GVRP

GARP VLAN Registration Protocol (GVRP) allows the exchange of VLAN information between switches in a network. If one switch is manually configured with multiple VLANs, other switches in the network learn about these VLANs dynamically through GVRP.

To configure GVRP, you must enable GVRP on ports on each end of the trunk. Add a VLAN bridge (2) and enable spanning tree protocol on this bridge and specify the VLAN as active. This active state allows forwarding of frames on this VLAN. Set GVRP globally for this bridge. Associate interfaces with this bridge and specify switching characteristics according to requirement

This configuration sample assumes that you are running the SRstackware Layer 2 module. If you are using the SRstackware Hybrid Layer 2/Layer 3 module, run the switchport command on each port to set the switching characteristics of Layer 2 protocols.

Figure 9-1 GVRP Configuration

Bridge 2	
# configure terminal	Enter the Configure mode.
(config)# bridge 2 protocol ieee vlan-bridge	Specify VLAN for bridge 2.
(config)# vlan database	Enter the VLAN configuration mode.
(config-vlan)# vlan 5 bridge 2 state enable	Enable the state of a particular VLAN (5) on bridge 2.
(config-vlan)# exit	Exit the VLAN configuration mode and enter Configure mode.
(config)# interface eth2	Specify the interface (eth2) to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth2 with bridge group 2.

Bridge 2	
(config-if)# switchport mode trunk	Set the switching characteristics of the Layer 2 interface as trunk and specify tagged frames only. Set the ingress filtering for received frames. Received frames that are not classified as trunk are discarded.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# set gvrp enable bridge 2	Set GVRP globally for bridge 2.
(config)# set port gvrp enable eth2	Enable GVRP on port eth2.
(config)# set gvrp dynamic-vlan-creation enable bridge 2	Enable dynamic VLAN creation for this bridge instance.
(config)# interface eth4	Specify the interface (eth4) to be configured and enter the Interface mode.
(config-if)# bridge-group 2	Associate the interface eth3 with bridge group 2.
(config-if)# switchport mode access	Use this command to set the switching characteristics of the Layer 2 interface to access mode
(config-if)# switchport access vlan 5	Use this command to change the default VLAN ID to 5 on eth4.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.

Bridge 3	
# configure terminal	Enter the Configure mode.
(config)# bridge 3 protocol ieee vlan-bridge	Specify VLAN for bridge 3.
(config)# interface eth2	Specify the interface (eth2) to be configured and enter the Interface mode.
(config-if)# bridge-group 3	Associate the interface eth3 with bridge group 3.
(config-if)# exit	Exit the Interface mode and enter the Configure mode.
(config)# set gvrp enable bridge 3	Set GVRP globally for bridge 3.
(config)# set port gvrp enable eth2	Enable GVRP on port eth2.

Bridge 3	
(config)# set gvrp dynamic-vlan-creation enable bridge 3	Enable dynamic VLAN creation for this bridge instance.
(config-if)# switchport mode trunk	Set the switching characteristics of the Layer 2 interface as trunk and specify tagged frames only. Set the ingress filtering for received frames. Received frames that are not classified as trunk are discarded.

Names of Commands Used

`bridge protocol vlan-bridge, bridge-group, bridge spanning-tree enable, switchport mode trunk, vlan bridge, switchport trunk allowed vlan`

Validation Commands

`show gvrp configuration, show gvrp timer`

QoS Configuration

10.1 Introduction

This chapter contains:

- An overview of QoS functionality and terminology
- A QoS configuration example for a relevant scenario
- Configuration guidelines
- Sample procedures for enabling and configuring QoS

To see details on the commands used in this chapter, refer to the *SRstackware® Intelligent Network Software Switch Configuration Command Reference*.

The main requirement is to enable and configure QoS on the desired switch.

10.2 QoS Functionality

Quality of Service (QoS) can be used to give certain traffic priority over other traffic.

Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped.

With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

QoS is based on DiffServ architecture which stipulates that individual packets are classified upon entry into a network. Classification information can be carried in the Layer 3 IP packet header or the Layer 2 frame. IP packet headers carry the information using 6 bits from the deprecated IP type of service (TOS) field. Layer 2 802.1Q frames carry the information using a 2-byte Tag Control Information field.

All switches and routers accessing the Internet depend on class information to give the same forwarding treatment to packets with the same class information, and give different treatment to packets with different class information. A packet can be assigned class information, as follows:

- End hosts or switches along a path, based on a configured policy
- Detailed packet examination, expected to occur nearer to the network edge, to prevent overloading core switches and routers
- A combination of the above two techniques

Class information can be used by switches and routers along a path to limit the amount of allotted resources per traffic class.

Per-hop behavior is an individual device's behavior when handling traffic in the DiffServ architecture. An end-to-end QoS solution can be created if all devices along a path have consistent per-hop behavior.

10.3 Terminology

Following is a brief description of terms and concepts used to describe QoS.

10.3.1 ACL

Access control lists (ACLs) classify traffic with the same characteristics. IP traffic is classified using IP standard or IP extended ACLs.

The ACL can have multiple Access Control Entries (ACEs), which are commands that match fields against the contents of the packet.

It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS, but it is possible to match IP options against configured IP extended ACLs to enforce QoS.

10.3.2 Cos Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer 2 frames upon entry into a network.

QoS classifies frames by assigning priority-indexed CoS values to them and gives preference to higher-priority traffic.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the 3 most significant bits, called the User Priority bits. On interfaces configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames, except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

CoS values range from 0 to 7, 7 being the highest priority.

10.3.3 DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer 3 packets upon entry into a network.

DSCP values range from 0 to 63, 63 being the highest priority, 0 being best-effort traffic.

10.3.4 Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet. The process generates an internal DSCP for a packet, which identifies all future QoS actions to be taken on the packet.

Each packet is classified upon entry into the network. At the ingress, the packet is inspected, and the DSCP is determined based on ACLs or the configuration. The Layer 2 CoS value is then mapped to a DSCP value.

The classification is carried in the IP packet header using 6 bits from the deprecated IP TOS field to carry the classification information. Classification can also occur in the Layer 2 frame.

Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, thus, no classification occurs.

Classification occurs on an ingress physical port, but not at the switch virtual interface level.

Classification can be based on QoS ACLs, or class maps and policy maps.

10.3.5 Policing

Policing determines whether a packet is in or out of profile by comparing the internal DSCP to the configured policer. The policer limits the bandwidth consumed by a traffic flow. The result is given to the marker.

There are two types of policers:

- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.
- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, the aggregate policer is shared by multiple classes of traffic within a policy map.

Policing and policers have the following attributes:

- Policers can occur only on a physical port basis
- Policing can occur on ingress interfaces
- Only one policer can be applied to a packet per direction

10.3.6 Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration information to determine the action required for the packet, then handles the packet using one of the following methods:

- Let the packet through without modification
- Drop the packet

Marking can occur on ingress and egress interfaces.

10.3.7 Queueing

Queueing maps packets to a CoS queue. Each egress port can accommodate up to eight CoS queues, prioritized as 0 lowest and 7 highest.

The tagged packet incoming priority can be mapped to one of the eight queues obtained from the filtering mechanism result. The untagged packet CoS priority is also obtained from the filtering mechanism result.

After the packets are mapped to a CoS queue, they are scheduled.

10.3.8 Scheduling

Scheduling forwards or conditions packets using one of the following methods:

Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted.

Weighted Round Robin (WRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.

Combination of WRR and SP, in which both methods are used. The weight of one or more of the CoS queues can be set to 0. Other queues are set to weights other than 0. Packets in weight-0 queues are sent first if there are packets in those queues. If there are not any packets in the weight-0 queues, packets are sent from other queues using the WRR method. If a packet arrives in a weight-0 queue, WRR scheduling is preempted, and the packet is sent from the weight-0 queue. If no more packets arrive from weight-0 queues, WRR queueing is resumed.

10.3.9 Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it.

The criteria can include:

- Matching the access group defined by the ACL
- Matching a specific list of DSCP values

If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class map criteria, it is further classified using a policy map.

10.3.10 Policy Map

A policy map specifies on which traffic class to act. This can be implemented as follows:

- Set a specific CoS or DSCP value in the traffic class
- Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile

Policy maps have the following attributes:

- A policy map can contain multiple class statements, each with different match criteria and policers
- A separate policy map class can exist for each type of traffic received through an interface
- There can be only one policy map per interface per direction, the same policy map can be applied to multiple interfaces and directions
- Before a policy map can be effective, it must be attached to an interface

10.3.11 Mapping Tables

QoS uses configurable mapping tables during classification. The DSCP-to-CoS map and the DSCP-to-DSCP mutation map are supported.

10.3.12 DSCP-to-CoS Map

The DSCP-to-CoS map is used to generate a CoS value to select one of the eight egress queues.

10.3.13 DSCP-to-DSCP-Mutation Map

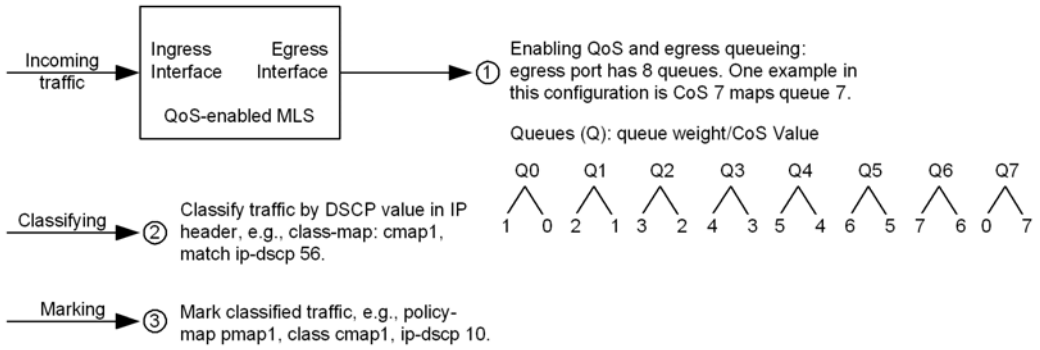
The DSCP-to-DSCP-mutation map applies to a port at an QoS administrative domain boundary if the two domains have different DSCP definitions between them. In this way, the map translates a DSCP value set that matches the other domain's definition.

The default DSCP-to-DSCP-mutation map is null, and maps an incoming DSCP value to the same DSCP value.

10.4 Configuration Example

The following example shows a DSCP value of 56, a CoS value of 7, with CoS 7 mapped to queue 7.

Figure 10-1 QoS Configuration



10.5 Configuration Guidelines

The following provides information to consider before configuring QoS:

- QoS policing cannot be configured over EtherChannel
- Traffic can be classified per ingress port or per port-per-VLAN
- There can be only one ACL configuration command per class map. An ACL can have multiple commands (access control entries) that match fields against the packet contents.
- Policing cannot be done at the switch virtual interface level, a policer can be configured on an ingress physical port
- As a part of egress queue configuration, define which packets identified by the CoS value, get assigned to one of the eight egress queues.

10.6 Sample Procedures

The following subsections provide examples of how to enable and configure QoS.

Commands are indicated in **`bold Courier`** type. Parameters are indicated in `plain Courier` type. Additional information is indicated in Arial type.

10.6.1 Enable QoS

Enabling QoS involves assigning weights to the egress queues, and mapping CoS values to the egress queues.

To enable QoS, enter the following commands from Privileged Exec mode.

1. **configure terminal**.
2. **mls QoS** `QUEUE_WEIGHT COS_VALUE` to enable QoS globally.
   `QUEUE_WEIGHT` = weight of each of the 8 egress queues; range is 0-10
   `COS_VALUE` = CoS values mapped to each of the 8 egress queues; range is 0-7

NOTE: The `no mos qos` command disables QoS.

The following example shows enabling QoS.

```
Router_C# configure terminal
Router_C(config)# mls QoS 1 0 2 1 3 2 4 3 5 4 6 5 7 6 0 7
```

10.6.2 Configure Policy

To configure a QoS policy, the following is usually required:

- Categorize traffic into classes
- Configure policies to apply to the traffic classes
- Attach policies to interfaces

10.6.2.1 Classify Traffic Using ACLs

IP traffic can be classified using IP standard or IP extended ACLs.

The following shows creating an IP standard ACL for IP traffic. Follow these steps from Privileged Exec mode.

1. **`configure terminal`**.
2. `ip-access-list ACCESS-LIST NUMBER deny|permit SOURCE (SOURCE WILDCARD)` to create an IP standard ACL. Repeat this step as needed.

`ACCESS-LIST NUMBER` range is 1-99 and 1300-1999

`deny` = deny certain traffic if conditions matched

`permit` = permit certain traffic if conditions matched

`SOURCE` = originating network or host sending packet. The word, any, can be used in place of 0.0.0.0 255.255.255.255.

`SOURCE WILDCARD` = optional. Wild card bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.

NOTE: The no `ip-access-list` command deletes an access list.

The following example shows allowing access only for hosts on three specified networks. Wildcard bits correspond to the network address host portions. If a host has a source address that does not match the access list statements, it is rejected.

```
Router_C(config)# ip-access-list 1 permit 192.5.255.0
0.0.0.255

Router_C(config)# ip-access-list 1 permit 128.88.0.0
0.0.255.255

Router_C(config)# ip-access-list 1 permit 36.0.0.0
0.0.0.255
```

10.6.2.2 Classify Traffic on Physical-Port Basis

The following shows classifying IP standard traffic on a physical-port basis using class maps. This involves creating a class map, and defining the match criterion.

1. **`configure terminal`**.
2. `ip-access-list ACCESS-LIST NUMBER deny|permit SOURCE (SOURCE WILDCARD)` to create an IP standard ACL.

   `ACCESS-LIST NUMBER` range is 1-99 and 1300-1999

   `deny` = deny certain traffic if conditions matched

   `permit` = permit certain traffic if conditions matched

   `SOURCE` = originating network or host sending packet. The word, any, can be used in place of 0.0.0.0 255.255.255.255.

   `SOURCE WILDCARD` = optional. Wild card bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.

NOTE: The end of the access list, by default, has an implied deny statement for everything if it does not locate a match before reaching the end.

3. **class-map** NAME to create a class map.
   NAME = name of the class map.

NOTE: All match criteria in the class map must be matched.

4. match access-group NAME to define the match criterion.
   NAME = number or name of the ACL created using the ip-access-list command.

NOTE: The no class-map command deletes an existing class-map.

The following example shows configuring a class map named cmap1 with 1 match criterion: access list 103, which allows traffic from any source to any destination.

```
Router_C(config)# ip-access-list 103 permit ip any any
Router_C(config)# class-map cmap1
Router_C(config-cmap)# match access-group 103
```

10.6.2.3 Classify Traffic on a Per-Port-Per-VLAN Basis

The following shows classifying traffic on a per-port-per-VLAN basis using class maps. This involves creating a class map, and defining the match criterion.

1. **configure terminal**.
2. **class-map** NAME to create a class map.
   NAME = name of the class map.
3. match ip-dscp LIST.
   LIST = list to match against incoming packets. Up to eight IP DSCP values separated by a space. Range is 0-63.
4. match vlan-range <1-4022> to <1-4022>.
5. exit.

The following example shows configuring a class map named cmap1 with criterion that matches IP DSCP 56.

```
Router_C(config)# class-map cmap1
Router_C(config-cmap)# match ip-dscp 56
Router_C(config-cmap)# match vlan-range 20 to 30
Router_C(config-cmap)# exit
```

10.6.2.4 Create Policy Map

The following shows creating a policy map to classify, police, and mark traffic.

1. **`configure terminal`**
2. **`ip-access-list`** `ACCESS-LIST NUMBER` **`deny|permit`** `SOURCE (SOURCE WILDCARD)` to create an IP standard ACL.
3. **`class-map`** `NAME` to create a class map.

   `NAME` = name of the class map.
4. **`policy-map`** `NAME` to create a policy map.

   `NAME` = name of the policy map.
5. **`class NAME`** to define a traffic classification.

   `NAME` = name of the class map.
6. `set cos|ip-dscp` to set a new value in the packet to classify IP traffic.

   `cos` = new CoS value to assign to classified traffic. Range is 0-7.

   `ip-dscp` = new DSCP value to assign to classified traffic. Range is 0-63.
7. **`police`** `RATE BURST (`**`exceed action drop`**`)` to specify a policer. Up to 128 policers can be configured on ingress Gigabit-capable Ethernet ports, and up to eight on ingress 10/100 Ethernet ports and egress ports.

   `RATE` = average traffic rate in bps. Range is 1-1000000.

   `BURST` = normal burst size in kilobytes. Range is 1-20000.

   `exceed action drop =` optional parameter which specifies dropping the packet when rates are exceeded.
8. **`exit`**.
9. **`exit.`**
10. **`interface`** `IFNAME` to specify the interface to match to the policy map.
11. `service-policy input INPUT NAME` to apply a policy map to the input of the specified interface.

    `INPUT NAME` = policy-map name to apply the specified policy-map to the interface input.

There can be only one policy map per interface.

The no policy-map command deletes an existing policy-map. The no set cos|dscp command removes a specified CoS or DSCP value. The no police command removes an existing policer. The no service-policy input command removes a policy map and interface association.

The following example shows creating a policy map, and attaching it to an ingress interface. In this example, the IP standard ACL allows traffic from network 10.1.0.0. If the matched traffic exceeds a 48000-bps average traffic rate and a 8000-kilobyte normal burst size, its DSCP is marked down, and sent.

```
Router_C(config)# ip-access-list 1 permit 10.1.0.0 0.0.255.255
Router_C(config)# class-map cmap1
Router_C(config-cmap)# match access-group 1
Router_C(config-cmap)# exit
Router_C(config)# policy-map pmap1
Router_C(config-pmap)# class cmap1
Router_C(config-pmap-c)# police 48000 8000 exceed-action drop
Router_C(config-pmap-c)# exit
Router_C(config-pmap)# exit
Router_C(config)# interface ge1
Router_C(config-if)# service-policy input pmap1
```

10.6.2.5 Create Aggregate Policer

The following shows creating an aggregate policer to classify, police, and mark traffic.

1. **`configure terminal`**.
2. `mls qos aggregate-police NAME RATE BURST (exceed action drop)` to specify policer parameters to apply to multiple traffic classes in the same policy-map.

   `NAME` = name of the aggregate policer.

   `RATE` = average traffic rate in bps. Range is 1-1000000.

   `BURST` = normal burst size in kilobytes. Range is 1-20000.

   `exceed action` = optional parameter which specifies action required for packet when rates are exceeded.

   `drop` = drop the packet.
3. **`class-map`** NAME to create a class map.

   `NAME` = name of the class map.
4. **`policy-map`** NAME to create a policy map.

   `NAME` = name of the policy map.
5. **`class`** NAME to define a traffic classification.

   `NAME` = name of the class map.
6. `police-aggregate NAME` to apply the previously named aggregate policer to multiple classes in the same policy-map.

`NAME =` name of the aggregate policer issued in the mls qos aggregate-police command previously in this procedure.

7. **`exit`**.
8. `interface IFNAME` to specify the interface to attach to the policy map.
9. `service-policy input INPUT NAME` to apply the policy map to the input of the specified interface.

   `INPUT NAME =` policy map name to apply the specified policy-map to the interface input.

NOTE: There can be only one policy map per interface.

The no police-aggregate command deletes an aggregate policer from a policy map. The no `mls qos aggregate-police` command deletes an aggregate policer, along with its parameters.

The following example shows creating an aggregate policer, and attaching it to multiple classes within a policy map. In this example, the IP ACLs allow traffic from network 10.1.0.0 and host 11.3.1.1. The traffic rate from network 10.1.0.0 and host 11.3.1.1 is policed. If the traffic exceeds a 48000-bps average traffic rate and a 8000-kilobyte normal burst size, it is considered out of profile, and is dropped. The policy map is attached to an ingress interface.

```
Router_C(config)# ip-access-list 1 permit 10.1.0.0 0.0.255.255
Router_C(config)# ip-access-list 2 permit 11.3.1.1
Router_C(config)# mls qos aggregate-police transmit1 48000 8000
exceed-action drop
Router_C(config)# class-map cmap1
Router_C(config-cmap)# match access-group 1
Router_C(config-cmap)# exit
Router_C(config)# class-map cmap2
Router_C(config-cmap)# match access-group 2
Router_C(config-cmap)# exit
Router_C(config)# policy-map aggflow1
Router_C(config-pmap)# class-map cmap1
Router_C(config-pmap-c)# police-aggregate transmit1
Router_C(config-pmap-c)# exit
Router_C(config-pmap)# class-map cmap2
Router_C(config-pmap-c)# set ip-dscp 56
Router_C(config-pmap-c)# police-aggregate transmit1
Router_C(config-pmap-c)# exit
```

```
Router_C(config-pmap)# exit
Router_C(config)# interface ge1
Router_C(config-if)# service-policy input aggflow1
Router_C(config-if)# exit
```

10.6.3 Configure DSCP Maps

Multiple DSCP-to-DSCP mutation maps can be applied to different Gigabit-capable Ethernet ports.

10.6.3.1 DSCP-to-CoS Map

The following shows modifying a DSCP-to-CoS map. This map is used to generate a CoS value, this value selects one of the eight egress queues.

1. **`configure terminal`**.
2. `mls qos map dscp-cos UNIT-NAME LIST` **`to`** `VALUE` to modify the DSCP-to-CoS map.

   `UNIT-NAME` = name of unit.

   `LIST` = up to eight DSCP values, each separated by a space. Range is 0-63.

   `VALUE` = CoS value: DSCP values correspond to this value. Range is 0-7.

NOTE: The no mls qos map dscp-cos UNIT-NAME command removes a configured DSCP-to-CoS mapping table.

The following example shows mapping DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0.

```
Router_C# configure terminal
Router_C(config)# mls qos map dscp-cos base 0 8 16 24 32 40 48 50
to 0
```

10.6.3.2 DSCP-to-DSCP Mutation Map

The following shows modifying a DSCP-to-DSCP mutation map. This map is used if two domains have different DSCP definitions; this map translates a set of one domain's DSCP values to match the other domain's definition. The default DSCP-to-DSCP mutation map maps an incoming DSCP value to the same DSCP value.

1. **`configure terminal`**.
2. `mls qos map dscp-mutation UNIT_NAME IN_DSCP to OUT_DSCP` to revise the DSCP-to-DSCP mutation map.

   `UNIT_NAME` = name of unit

`IN_DSCP` = eight DSCP values separated by spaces; range is 0-63

`OUT_DSCP` = single DSCP value; range is 0-63

NOTE: The no `mls qos map dscp-mutation` command returns to the default map.

The following example shows defining a DSCP-to-DSCP mutation map.

```
Router_C# configure terminal
Router_C(config)# mls qos map dscp-mutation base 1 2 3 4 5 6 7 to 0
Router_C(config)# mls qos map dscp-mutation base 8 9 10 11 12 13 to 10
Router_C(config)# mls qos map dscp-mutation base 20 21 22 to 20
Router_C(config)# mls qos map dscp-mutation base 30 31 32 33 34 to 30
```

10.7 Verify QoS Information

Use the following commands to verify QoS information.

10.7.1 Class Maps

The show `class-map` command displays the QoS class-maps to define the match criteria to classify traffic.

```
Router_C# show class-map cmap1

    CLASS-MAP-NAME: cmap1

      Set IP DSCP: 56

      Match IP DSCP: 7
```

10.7.2 Aggregate Policer Configuration

The show `mls qos aggregate-policer` command displays the aggregate policer configuration.

```
Router_C#show mls qos aggregate-policer agp1

 AGGREGATOR-POLICER-NAME: agp1

   Police:   Average rate(1 kbps), burst size(1 bytes)  Exceed-action drop
```

10.7.3 QoS Mapping Information

The show mls qos maps command displays QoS mapping information.

```
Router_C#show mls qos maps dscp-cos base
  DSCP-TO-COS-MAP:  base

DSCP-TO-COS-MAP:  base
d1 d2 0  1  2  3  4  5  6  7  8  9
0     4  4  4  4  4  4  4  4  1  1
1     1  1  1  1  1  1  2  2  2  2
2     2  2  2  2  3  3  3  3  3  3
3     3  3  4  4  4  4  4  4  4  4
4     5  5  5  5  5  5  5  5  6  6
5     6  6  6  6  6  6  7  7  7  7
6     7  7  7  7

Router_C#show mls qos maps dscp-mutation base

DSCP-TO-DSCP-MUTATION-MAP:  base
d1 d2 0  1  2  3  4  5  6  7  8  9
0     0  1  2  3  4  5  6  7  8  9
1     4  4  4  4  4  4  4  17 18 19
2     20 21 22 23 24 25 26 27 28 29
3     30 31 32 33 34 35 36 37 38 39
4     40 41 42 43 44 45 46 47 48 49
5     50 51 52 53 54 55 56 57 58 59
6     60 61 62 63
```

10.7.4 QoS Policy-Map Information

The show policy-map command displays QoS policy-map information.

```
Router_C#show policy-map mapa class pmap1
  POLICY-MAP-NAME: pmap1
    State: detached
    CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
```

Validation Commands Sample Output

A.1 Overview

This appendix provides the sample outputs of the validation commands for STP, RSTP, VLAN, LACP, and IGMP Snooping configurations.

The outputs provided in this section are generated using a sample configuration on a reference platform.

A.2 STP Configuration

A.2.1 show spanning-tree

```
atca-blade#show spanning-tree interface xe9
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 800000a34f060003
% 1: Bridge Id 800000a34f060003
% 1: last topology change Thu May  5 11:53:54 2011
% 1: 1 topology change(s)  - last topology change Thu May  5 11:53:54 2011
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%  xe9: Port Number 925 - Ifindex 5021 - Port Id 839d - Role Designated
- State Forwarding
%   xe9: Designated Path Cost 0
%   xe9: Configured Path Cost 4  - Add type Explicit ref count 1
%   xe9: Designated Port Id 839d - Priority 128  -
%   xe9: Root 800000a34f060003
%   xe9: Designated Bridge 800000a34f060003
%   xe9: Message Age 0 - Max Age 20
%   xe9: Hello Time 2 - Forward Delay 15
%  xe9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   xe9: forward-transitions 1
%   xe9: Version Spanning Tree Protocol  - Received None - Send STP
%   xe9: No portfast configured - Current  portfast off
%  xe9: portfast bpdu-guard  default  - Current portfast bpdu-guard off
```

```
%  xe9: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe9: no root guard configured     - Current root guard off
%   xe9: Configured Link Type point-to-point - Current point-to-point
%
```

A.2.2 show bridge

```
atca-blade#show bridge
bridge CVLAN SVLAN BVLAN      port             mac        fwd timeout
1        21 xe9               0080.422b.9a79    1             300
```

A.3 RSTP Configuration

A.3.1 show spanning-tree

```
atca-blade#show spanning-tree interface xe9

% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 800000752bfc0003
% 1: Bridge Id 800000752bfc0003
% 1: last topology change Wed May  4 11:22:56 2011
% 1: 1 topology change(s)  - last topology change Wed May  4 11:22:56 2011
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%  xe9: Port Number 925 - Ifindex 5021 - Port Id 839d - Role Designated
- State Forwarding
%   xe9: Designated Path Cost 0
%    xe9: Configured Path Cost 20000  - Add type Explicit ref count 1
%   xe9: Designated Port Id 839d - Priority 128  -
%   xe9: Root 800000752bfc0003
%   xe9: Designated Bridge 800000752bfc0003
%   xe9: Message Age 0 - Max Age 20
%   xe9: Hello Time 2 - Forward Delay 15
%  xe9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   xe9: forward-transitions 1
%  xe9: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   xe9: No portfast configured - Current  portfast off
```

```
%   xe9: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   xe9: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe9: no root guard configured      - Current root guard off
%   xe9: Configured Link Type point-to-point - Current point-to-point
```

A.3.2 show bridge

atca-blade#show bridge

```
bridge      CVLAN SVLAN     BVLAN       port          mac        fwd timeout
1                 22         xe9     0018.4900.429b     1                300
```

A.4 MSTP Configuration

A.4.1 show spanning-tree mst instance

atca-blade#show spanning-tree mst instance 1

```
 % 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768

% 1: MSTI Root Id 80010072e11c000f

% 1: MSTI Bridge Id 80010072e11c000f

%  xe10: Port Number 918 - Ifindex 5014 - Port Id 8396 - Role Masterport
- Stat

e Forwarding

%   xe10: Designated Internal Path Cost 0  - Designated Port Id 8396

%   xe10: Configured Internal Path Cost 2000

%   xe10: Configured CST External Path cost 2000

%   xe10: CST Priority 128  - MSTI Priority 128

%   xe10: Designated Root 80010072e11c000f

%   xe10: Designated Bridge 80010072e11c000f

%   xe10: Message Age 0 - Max Age 0

%   xe10: Hello Time 2 - Forward Delay 15

%   xe10: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%
```

```
%   xe9: Port Number 917 - Ifindex 5013 - Port Id 8395 - Role Disabled -
State Discarding

%   xe9: Designated Internal Path Cost 0  - Designated Port Id 0

%   xe9: Configured Internal Path Cost 2000

%   xe9: Configured CST External Path cost 2000

%   xe9: CST Priority 128  - MSTI Priority 128

%   xe9: Designated Root 00000072e11c000f

%   xe9: Designated Bridge 00000072e11c000f

%   xe9: Message Age 0 - Max Age 0

%   xe9: Hello Time 0 - Forward Delay 0

%   xe9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

A.4.2 show spanning-tree mst detail

atca-blade-14-255#show spanning-tree mst detail

```
% 1: Bridge up - Spanning Tree Enabled

% 1: CIST Root Path Cost 2002 - CIST Root Port 5014 -  CIST Bridge Priority
3276

8

% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20

% 1: CIST Root Id 000000e2b0c9001d

% 1: CIST Reg Root Id 80000072e11c0003

% 1: CIST Bridge Id 80000072e11c0003

% 1: 23 topology change(s)  - last topology change Sat Apr  9 16:18:35 2011

% 1: portfast bpdu-filter disabled

% 1: portfast bpdu-guard disabled

% 1: portfast errdisable timeout disabled

% 1: portfast errdisable timeout interval 300 sec

%   xe10: Port Number 918 - Ifindex 5014 - Port Id 8396 - Role Rootport -
State Forwarding
```

```
%   xe10: Designated External Path Cost 2 -Internal Path Cost 0

%   xe10: Configured Path Cost 2000  - Add type Explicit ref count 2

%   xe10: Designated Port Id 8396 - CIST Priority 128  -

%   xe10: CIST Root 000000e2b0c9001d

%   xe10: Regional Root 80000072e11c0003

%   xe10: Designated Bridge 800000581d4c0003

%   xe10: Message Age 1 - Max Age 20

%   xe10: CIST Hello Time 2 - Forward Delay 15

%   xe10: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo
change timer 0

%   xe10: forward-transitions 1

%  xe10: Version Multiple Spanning Tree Protocol - Received STP - Send STP

%   xe10: No portfast configured - Current  portfast off

%   xe10: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%  xe10: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe10: no root guard configured     - Current root guard off

%   xe10: Configured Link Type point-to-point - Current point-to-point

%

%   xe9: Port Number 917 - Ifindex 5013 - Port Id 8395 - Role Disabled -
State Discarding

%   xe9: Designated External Path Cost 0 -Internal Path Cost 0

%   xe9: Configured Path Cost 2000  - Add type Explicit ref count 2

%   xe9: Designated Port Id 0 - CIST Priority 128  -

%   xe9: Message Age 0 - Max Age 0

%   xe9: CIST Hello Time 0 - Forward Delay 0

%   xe9: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe9: forward-transitions 0

%   xe9: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP
```

```
%   xe9: No portfast configured - Current  portfast off
%   xe9: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   xe9: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe9: no root guard configured     - Current root guard off
%   xe9: Configured Link Type point-to-point - Current point-to-point
%
%   xe12: Port Number 920 - Ifindex 5016 - Port Id 8398 - Role Disabled -
State Discarding
%   xe12: Designated External Path Cost 0 -Internal Path Cost 0
%   xe12: Configured Path Cost 200000000  - Add type Explicit ref count 1
%   xe12: Designated Port Id 0 - CIST Priority 128  -
%   xe12: Message Age 0 - Max Age 0
%   xe12: CIST Hello Time 0 - Forward Delay 0
%   xe12: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   xe12: forward-transitions 0
%   xe12: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP
%   xe12: No portfast configured - Current  portfast off
%   xe12: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   xe12: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe12: no root guard configured     - Current root guard off
%   xe12: Configured Link Type point-to-point - Current point-to-point
%
%   xe11: Port Number 919 - Ifindex 5015 - Port Id 8397 - Role Disabled -
State
Discarding
%   xe11: Designated External Path Cost 0 -Internal Path Cost 0
%   xe11: Configured Path Cost 200000000  - Add type Explicit ref count 1
%   xe11: Designated Port Id 0 - CIST Priority 128  -
```

```
%   xe11: Message Age 0 - Max Age 0

%   xe11: CIST Hello Time 0 - Forward Delay 0

%   xe11: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe11: forward-transitions 0

%   xe11: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe11: No portfast configured - Current  portfast off

%   xe11: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe11: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe11: no root guard configured     - Current root guard off

%   xe11: Configured Link Type point-to-point - Current point-to-point

%

%   xe7: Port Number 915 - Ifindex 5011 - Port Id 8393 - Role Disabled -
State Forwarding

%   xe7: Designated External Path Cost 0 -Internal Path Cost 0

%   xe7: Configured Path Cost 2000  - Add type Explicit ref count 1

%   xe7: Designated Port Id 0 - CIST Priority 128  -

%   xe7: Message Age 0 - Max Age 0

%   xe7: CIST Hello Time 0 - Forward Delay 0

%   xe7: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe7: forward-transitions 1

%   xe7: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe7: No portfast configured - Current  portfast off

%   xe7: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe7: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe7: no root guard configured     - Current root guard off

%   xe7: Configured Link Type point-to-point - Current point-to-point
```

```
%

%   xe5: Port Number 913 - Ifindex 5009 - Port Id 8391 - Role Disabled -
State Discarding

%   xe5: Designated External Path Cost 0 -Internal Path Cost 0

%   xe5: Configured Path Cost 200000000  - Add type Explicit ref count 1

%   xe5: Designated Port Id 0 - CIST Priority 128  -

%   xe5: Message Age 0 - Max Age 0

%   xe5: CIST Hello Time 0 - Forward Delay 0

%   xe5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe5: forward-transitions 0

%   xe5: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe5: No portfast configured - Current  portfast off

%   xe5: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe5: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe5: no root guard configured     - Current root guard off

%   xe5: Configured Link Type point-to-point - Current point-to-point

%

%   xe6: Port Number 914 - Ifindex 5010 - Port Id 8392 - Role Disabled -
State Discarding

%   xe6: Designated External Path Cost 0 -Internal Path Cost 0

%   xe6: Configured Path Cost 200000000  - Add type Explicit ref count 1

%   xe6: Designated Port Id 0 - CIST Priority 128  -

%   xe6: Message Age 0 - Max Age 0

%   xe6: CIST Hello Time 0 - Forward Delay 0
%   xe6: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe6: forward-transitions 0

%   xe6: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP
```

```
%   xe6: No portfast configured - Current  portfast off
%   xe6: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   xe6: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe6: no root guard configured     - Current root guard off
%   xe6: Configured Link Type point-to-point - Current point-to-point
%
%   xe8: Port Number 916 - Ifindex 5012 - Port Id 8394 - Role Disabled -
State Forwarding
%   xe8: Designated External Path Cost 0 -Internal Path Cost 0
%   xe8: Configured Path Cost 2000  - Add type Explicit ref count 1
%   xe8: Designated Port Id 0 - CIST Priority 128  -
%   xe8: Message Age 0 - Max Age 0
%   xe8: CIST Hello Time 0 - Forward Delay 0
%   xe8: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   xe8: forward-transitions 1
%   xe8: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP
%   xe8: No portfast configured - Current  portfast off
%   xe8: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   xe8: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe8: no root guard configured     - Current root guard off
%   xe8: Configured Link Type point-to-point - Current point-to-point
%
%   xe3: Port Number 911 - Ifindex 5007 - Port Id 838f - Role Disabled -
State Discarding
%   xe3: Designated External Path Cost 0 -Internal Path Cost 0
%   xe3: Configured Path Cost 200000000  - Add type Explicit ref count 1
%   xe3: Designated Port Id 0 - CIST Priority 128  -
%   xe3: Message Age 0 - Max Age 0
```

```
%   xe3: CIST Hello Time 0 - Forward Delay 0

%   xe3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe3: forward-transitions 0

%   xe3: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe3: No portfast configured - Current  portfast off

%   xe3: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe3: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe3: no root guard configured     - Current root guard off

%   xe3: Configured Link Type point-to-point - Current point-to-point

%

%   xe1: Port Number 909 - Ifindex 5005 - Port Id 838d - Role Disabled -
State Forwarding

%   xe1: Designated External Path Cost 0 -Internal Path Cost 0

%   xe1: Configured Path Cost 2000  - Add type Explicit ref count 1

%   xe1: Designated Port Id 0 - CIST Priority 128  -

%   xe1: Message Age 0 - Max Age 0

%   xe1: CIST Hello Time 0 - Forward Delay 0

%   xe1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe1: forward-transitions 1

%   xe1: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe1: No portfast configured - Current  portfast off

%   xe1: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe1: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe1: no root guard configured     - Current root guard off

%   xe1: Configured Link Type point-to-point - Current point-to-point

%
```

```
%   xe2: Port Number 910 - Ifindex 5006 - Port Id 838e - Role Disabled -
State Forwarding

%   xe2: Designated External Path Cost 0 -Internal Path Cost 0

%   xe2: Configured Path Cost 2000  - Add type Explicit ref count 1

%   xe2: Designated Port Id 0 - CIST Priority 128  -

%   xe2: Message Age 0 - Max Age 0

%   xe2: CIST Hello Time 0 - Forward Delay 0

%   xe2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe2: forward-transitions 1

%   xe2: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe2: No portfast configured - Current  portfast off

%   xe2: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe2: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe2: no root guard configured     - Current root guard off

%   xe2: Configured Link Type point-to-point - Current point-to-point

%

%   ge3: Port Number 907 - Ifindex 5003 - Port Id 838b - Role Disabled -
State Forwarding

%   ge3: Designated External Path Cost 0 -Internal Path Cost 0

%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 1

%   ge3: Designated Port Id 0 - CIST Priority 128  -

%   ge3: Message Age 0 - Max Age 0

%   ge3: CIST Hello Time 0 - Forward Delay 0

%   ge3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   ge3: forward-transitions 1

%   ge3: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   ge3: No portfast configured - Current  portfast off
```

```
%   ge3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%
%   ge1: Port Number 905 - Ifindex 5001 - Port Id 8389 - Role Disabled -
State Forwarding
%   ge1: Designated External Path Cost 0 -Internal Path Cost 0
%   ge1: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge1: Designated Port Id 0 - CIST Priority 128  -
%   ge1: Message Age 0 - Max Age 0
%   ge1: CIST Hello Time 0 - Forward Delay 0
%   ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   ge1: forward-transitions 1
%   ge1: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP
%   ge1: No portfast configured - Current  portfast off
%   ge1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge1: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   ge1: no root guard configured     - Current root guard off
%   ge1: Configured Link Type point-to-point - Current point-to-point
%
%   ge2: Port Number 906 - Ifindex 5002 - Port Id 838a - Role Disabled -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 0
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0 - CIST Priority 128  -
%   ge2: Message Age 0 - Max Age 0
%   ge2: CIST Hello Time 0 - Forward Delay 0
```

```
%   ge2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   ge2: forward-transitions 1

%   ge2: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   ge2: No portfast configured - Current  portfast off

%   ge2: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   ge2: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   ge2: no root guard configured     - Current root guard off

%   ge2: Configured Link Type point-to-point - Current point-to-point

%

%   ge4: Port Number 908 - Ifindex 5004 - Port Id 838c - Role Disabled -
State Forwarding

%   ge4: Designated External Path Cost 0 -Internal Path Cost 0

%   ge4: Configured Path Cost 20000  - Add type Explicit ref count 1

%   ge4: Designated Port Id 0 - CIST Priority 128  -

%   ge4: Message Age 0 - Max Age 0

%   ge4: CIST Hello Time 0 - Forward Delay 0

%   ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   ge4: forward-transitions 1

%   ge4: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   ge4: No portfast configured - Current  portfast off

%   ge4: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   ge4: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   ge4: no root guard configured     - Current root guard off

%   ge4: Configured Link Type point-to-point - Current point-to-point

%

%   xe4: Port Number 912 - Ifindex 5008 - Port Id 8390 - Role Disabled -
State Discarding
```

```
%   xe4: Designated External Path Cost 0 -Internal Path Cost 0

%   xe4: Configured Path Cost 200000000  - Add type Explicit ref count 1

%   xe4: Designated Port Id 0 - CIST Priority 128  -

%   xe4: Message Age 0 - Max Age 0

%   xe4: CIST Hello Time 0 - Forward Delay 0

%   xe4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0

%   xe4: forward-transitions 0

%   xe4: Version Multiple Spanning Tree Protocol - Received None - Send
MSTP

%   xe4: No portfast configured - Current  portfast off

%   xe4: portfast bpdu-guard  default  - Current portfast bpdu-guard off

%   xe4: portfast bpdu-filter default  - Current portfast bpdu-filter off

%   xe4: no root guard configured     - Current root guard off
%   xe4: Configured Link Type point-to-point - Current point-to-point

%

% Instance  1:  Vlans: 5

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768

% 1: MSTI Root Id 80010072e11c000f

% 1: MSTI Bridge Id 80010072e11c000f

%  xe10: Port Number 918 - Ifindex 5014 - Port Id 8396 - Role Masterport
- Stat

e Forwarding

%   xe10: Designated Internal Path Cost 0  - Designated Port Id 8396

%   xe10: Configured Internal Path Cost 2000

%   xe10: Configured CST External Path cost 2000

%   xe10: CST Priority 128  - MSTI Priority 128

%   xe10: Designated Root 80010072e11c000f

%   xe10: Designated Bridge 80010072e11c000f

%   xe10: Message Age 0 - Max Age 0
```

```
%   xe10: Hello Time 2 - Forward Delay 15

%   xe10: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

%   xe9: Port Number 917 - Ifindex 5013 - Port Id 8395 - Role Disabled -
State Discarding

%   xe9: Designated Internal Path Cost 0  - Designated Port Id 0

%   xe9: Configured Internal Path Cost 2000

%   xe9: Configured CST External Path cost 2000

%   xe9: CST Priority 128  - MSTI Priority 128
%   xe9: Designated Root 00000072e11c000f

%   xe9: Designated Bridge 00000072e11c000f

%   xe9: Message Age 0 - Max Age 0

%   xe9: Hello Time 0 - Forward Delay 0

%   xe9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

A.5 VLAN Configuration

A.5.1 show vlan all bridge

atca-blade#show vlan all bridge 1

```
ATCA-9305-14-255#show vlan all bridge 1
Bridge          VLAN ID  Name                            State   Member ports
                                                                 (u)-Untagged, (t)-Tagged
=============== ======= ============================== ======= ==============================
1               1        default                        ACTIVE  ge4(u)
1               2        VLAN02                         ACTIVE  xe1(u) xe5(u) xe6(u)
1               3        VLAN03                         ACTIVE  xe8(u) xe11(u) xe12(u)
1               5        VLAN0005                       ACTIVE  xe9(u) xe10(u)
1               11       VLAN11                         ACTIVE  xe2(u) xe4(u)
1               12       VLAN12                         ACTIVE  xe3(u) xe7(u)
1               21       VLAN21                         ACTIVE  ge1(u)
1               22       VLAN22                         ACTIVE  ge2(u)
ATCA-9305-14-255#
ATCA-9305-14-255#
```

A.5.2 show spanning-tree

atca-blade#show spanning-tree interface xe9

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 800000752bfc0003
% 1: Bridge Id 800000752bfc0003
% 1: last topology change Wed May  4 11:52:31 2011
% 1: 2 topology change(s)  - last topology change Wed May  4 11:52:31 2011
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   xe9: Port Number 925 - Ifindex 5021 - Port Id 839d - Role Designated
- State Forwarding
%   xe9: Designated Path Cost 0
```

```
%   xe9: Configured Path Cost 4  - Add type Explicit ref count 1
%   xe9: Designated Port Id 839d - Priority 128  -
%   xe9: Root 800000752bfc0003
%   xe9: Designated Bridge 800000752bfc0003
%   xe9: Message Age 0 - Max Age 20
%   xe9: Hello Time 2 - Forward Delay 15
%   xe9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   xe9: forward-transitions 1
%   xe9: Version Spanning Tree Protocol  - Received None - Send STP
%   xe9: No portfast configured - Current  portfast off
%   xe9: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   xe9: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   xe9: no root guard configured     - Current root guard off
%   xe9: Configured Link Type point-to-point - Current point-to-point
%
```

A.5.3 show vlan classifier group

atca-blade#show vlan classifier group

```
vlan classifier group 1 add rule 1
vlan classifier group 1 add rule 2
```

A.5.4 show vlan classifier rule

atca-blade#show vlan classifier rule

```
vlan classifier rule 1 ipv4 1.1.1.1/24 vlan 5
vlan classifier rule 2 proto ipv6 encap ethv2 vlan 5
```

A.6 LACP Configuration

A.6.1 show lacp sys-id

atca-blade#show lacp sys-id

```
% System 4e20,00-c3-0c-18-00-03
```

A.6.2 show etherchannel detail

atca-blade#show etherchannel detail

```
% Aggregator po10 1000000
% Mac address: 00:75:2b:fc:00:1b
% Admin Key: 0010 - Oper Key 0010
% Receive link count: 1 - Transmit link count: 0
% Individual: 0 - Ready: 1
% Partner LAG- 0x4e20,00-c3-0c-18-00-03
% Link: xe1 (5025) sync: 1
% Link: xe2 (5026) sync: 1
```

A.7 IGMP Snooping Configuration

A.7.1 show ip igmp interface vlan1.6

atca-blade#show ip igmp interface vlan1.6

```
Interface vlan1.6 (Index 17)

IGMP Enabled, Inactive, Version 3 (default)
IGMP interface has 0 group-record states
IGMP activity: 0 joins, 0 leaves
IGMP query interval is 125 seconds
IGMP Startup query interval is 31 seconds
IGMP Startup query count is 2
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Group Membership interval is 260 seconds
IGMP Last member query count is 2
Last member query response interval is 1000 milliseconds
IGMP Snooping is globally enabled
IGMP Snooping is not enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
```

A.7.2 show ip igmp groups

atca-blade#show ip igmp groups

```
IGMP Connected Group Membership

Group Address    Interface    Uptime     Expires      Last Reporter
239.1.2.3            ge3    00:00:34   00:03:45       192.168.5.1
```

A.8 GMRP Configuration

A.8.1 show gmrp configuration

```
atca-blade#show gmrp timer ge3

Timer           Timer Value (centiseconds)

----------------------------------------

Join                  20

Leave                 60

Leave All           1000
```

A.8.2 show gmrp configuration bridge 1

atca-blade#show gmrp configuration bridge 1

```
Global GMRP Configuration for bridge :1
GMRP Feature: Enabled

Port based GMRP Configuration:

                   Timers(centiseconds)

Port GMRP Status Registration  Forward All Join Leave  LeaveAll

-----------------------------------------------------------------------

ge3   Enabled        Normal      Enabled    20     60      1000
```

A.9 GVRP Configuration

A.9.1 show gvrp configuration

atca-blade#show gvrp configuration

```
Global GVRP Configuration for bridge 2:
Dynamic Vlan Creation: Disabled
Port based GVRP Configuration:


                Timers(centiseconds)
Port   GVRP Status  Registration   Applicant   Join   Leave   LeaveAll  -
------------------------------------------------------------------------
----
Global GVRP Configuration for bridge 1:
Dynamic Vlan Creation: Enabled
Port based GVRP Configuration:


                                Timers(centiseconds)
Port     GVRP Status  Registration   Applicant  Join  Leave  LeaveAll
------------------------------------------------------------------------
--------
ge3    Enabled        Normal           Normal      20     60      1000
```

A.9.2 show gvrp timer xe9

atca-blade#show gvrp timer xe9

```
Timer                Timer Value (centiseconds)
----------------------------------------
Join                      20
Leave                     60
Leave All                 1000
```

Related Documentation

B.1 SMART Embedded Computing Documentation

The documentation listed is referenced in this manual. Technical documentation can be found by using the Documentation Search at https://www.smartembedded.com/ec/support/ or you can obtain electronic copies of SMART EC documentation by contacting your local sales representative.

Table B-1 SMART Embedded Computing Publications

Document Title and Source	Publication Number
SRstackware Intelligent Network Software Troubleshooting Guide	6806800N83
SRstackware Intelligent Network Software VRRP Command Reference	6806800N84
SRstackware Intelligent Network Software RIP Command Reference	6806800N85
SRstackware Intelligent Network Software Layer 2 Command Reference	6806800N88
SRstackware Intelligent Network Software OSPF Command Reference	6806800N87
SRstackware Application Programming Interface Developer Guide	6806800N90
SRstackware Intelligent Network Software Layer 3 Configuration Guide	6806800N89
SRstackware Intelligent Network Software Switch Configuration Command Reference	6806800N92
SRstackware Intelligent Network Software Layer 3 Command Reference	6806800N93
SRstackware Intelligent Network Software Protocol Demo Guide	6806800N07
SRstackware FAQ	6806800N91

Related Documentation