SRstackware® Intelligent Network Software

Layer 2 Command Reference

P/N: 6806800N88G

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 The text itself may not be published commercially in print or electronic form, edited, translated, or otherwise altered without the permission of SMART EC.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

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 who install and configure SRstackware ARS IP routing software should use this manual.

This manual contains the following information:

An overview of the SRstackware Command Line Interface.

The complete command reference for these protocols and features: STP, RSTP, MSTP, 802.1x, VLAN, GVRP and GMRP.

This manual is divided into the following chapters and appendices.

Abbreviations

This document uses the following abbreviations:

Abbreviation	Definition
ASCII	American Standard Code for Information Interchange
BPDU	Bridge Protocol Data Units
CLI	Command Line Interface
GARP	Generic Attribute Registration Protocol
GID	GARP Information Declaration
GIP	GARP Information Propagation

Abbreviation	Definition
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
IGRP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Large Area Network
MST	Multiple Spanning Tree
MSTI	MST instance
MSTP	Multiple Spanning Tree Protocol
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree Protocol
STP	Spanning Tree Protocol
VRRP	Virtual Router Redundancy Protocol

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
<text>	Notation for variables and keys
[text]	Notation for software buttons to click on the screen and parameter description

Notation	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
Use ESD protection 	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
6806800N88G	April 2020	Rebranded to SMART Embedded Computing. Updated Abbreviations table.
6806800N88F	July 2017	Added registered trademark for SRstackware.
6806800N88E	June 2014	Rebranded to Artesyn template.
6806800N88D	August 2013	Added *Appendix 9, 802.1x Commands* .
6806800N88C	April 2013	Added *Bridge-group spanning-tree state on page 120*.
6806800N88B	October 2012	Added a note in *Chapter 8, IGMP Snooping Commands*.
6806800N88A	February 2012	EA Release

Command Line Interface Environment

1.1 Command Line Interface Primer

The SRstackware® Command Line Interface (CLI) is a text-based facility conforming to industry standards. Many of the commands may be used in scripts to automate configuration tasks. Each command CLI 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.

The IMI shell gives users and administrators the ability to issue commands to several daemons from a single telnet session.

1.1.1 Definitions

Definitions	
token	A non-character, non-numeric symbol: {}, {}, (), <>, |, ?, >, ., =
PARAMETER	An UPPERCASE term for which the user substitutes input.
keyword	A lowercase term that the user types exactly as shown.

1.1.2 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 a question mark ?. The SRstackware CLI displays the command keywords or parameters along with 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:

```
# 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
```

If the ? is typed in the middle of a keyword, SRstackware displays help for that keyword only.

> show de? (the CLI does not display the question mark).

```
debugging Debugging functions (see also 'undebug')
```

If the ? is typed in the middle of a keyword but the incomplete keyword matches several other keywords, SRstackware displays help for all matching keywords.

> show i? (the CLI does not display the question mark).

```
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

1.1.3 Syntax Help

1.1.3.1 Command Completion

The SRstackware CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press TAB. For example, at the CLI command prompt type sh:

```
> sh
```

Press TAB. The CLI shows:

```
> show
```

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

```
> show i
interface  ip   isis
> show i
```

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

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

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

```
> show interface
```

```
 IFNAME  Interface name
|       Output modifiers
 >       Output redirection
 <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

1.1.3.2 Command Abbreviations

The SRstackware CLI accepts abbreviations for commands. For example,

```
sh in eth0
```

is an abbreviation for the `show interface` command.

1.1.3.3 Command Line Errors

Any unknown spelling variation causes the command line parser to display in response to the ?, the error `Unrecognized command`. The parser redisplays the command as last entered. When the user presses the enter key after typing an invalid command, the parser displays:

```
(config)#router ospf here
                          ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

If a command is incomplete it displays this message:

```
> show
% Incomplete command.
```

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

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

1.2 Command Reference Primer

1.2.1 Typographic Conventions

The following table lists typographic conventions for command syntax descriptions.

Convention	Name	Description	Example
Monospaced font	Command	Represents command strings entered on a command line and sample source code.	`show ip ospf`
Proportional font	Description	Gives specific details about a parameter.	advertise Advertises this range
UPPERCASE	Variable parameter	Indicates user input. Values to be entered according to the descriptions that follow. Each uppercased token expands into one or more other tokens.	area AREAID range ADDRESS
lowercase	Keyword parameter	Indicates keywords. Values to be entered exactly as shown in the command description.	`show ip ospf`
|	Vertical bar	Delimits choices; One to be selected from the list. Not to be entered as part of the command.	A.B.C.D|<0-4294967295>
()	Parentheses	Encloses optional parameters. None or only one to be chosen. Not to be entered as part of the command.	(A.B.C.D|<0-4294967295>)
{ }	Braces	Encloses optional parameters. None, one or more than one to be chosen. Not to be entered as part of the command.	{priority <0-255>| poll-interval <1-65535>}
[]	Square brackets	Encloses optional parameters. Choose one. Not to be entered as part of the command.	[parm2|parm2|parm3]
?	Question mark	Used with the square brackets to limit the immediately following token to one occurrence. Not to be entered as part of the command.	[parm1|parm2|?parm3] expands to parm1 parm3 parm1 parm2 (with parm3 occurring once)

Convention	Name	Description	Example
< >	Angle brackets	Enclose a numeric range, endpoints inclusive. Not to be entered as part of the command.	<0-65535>
=	Equal sign	Separates the variable from explanatory text. Not to be entered as part of the command.	PROCESSID = <0-65535>
.	Dot (period)	Allows the repetition of the element that immediately follows it multiple times. Not to be entered as part of the command.	.AA:NN can be expanded to: 1:01 1:02 1:03.
A.B.C.D	IP address	An IPv4-style address.	10.0.11.123
X:X::X:X	IP address	An IPv6-style address.	3ffe:506::1, where the:: represents all 0s for those address components not explicitly given.
LINE	End-of-line input token	Indicates user input of any string, including spaces. No other parameters may be entered after input for this token.	string of words
WORD	Single token	Indicates user input of any contiguous string (excluding spaces).	singlewordnospaces
IFNAME	Single token	Indicates the name of an interface.	eth0

1.3 Format Used for Command Description

1.3.1 Command Name

Description of the command. What the command does and when should it be used.

1.3.1.1 Command Syntax

```
sample command name mandatory-parameters (OPTIONAL-PARAMETERS)
```

1.3.1.2 Default

The status of the command before it is executed. Is it enabled or disabled by default.

1.3.1.3 Command Mode

Name of the command mode in which this command is to be used. Such as, Exec, Privilege Exec, Configure mode and so on.

1.3.1.4 Usage

This section is optional. It describes the usage of a specific command and the interactions between parameters. It also includes appropriate sample outputs for `show` commands.

1.3.1.5 Example

Used if needed to show the complexities of the command syntax.

1.3.1.6 Related Commands

This section is optional and lists those commands that are of immediate importance.

1.3.1.7 Equivalent Commands

This section is optional and lists commands that accomplish the same function.

1.3.1.8 Validation Commands

This section is optional and lists commands that can be used to validate the effects of other commands.

1.3.2 Command Negation

Some commands can be negated by using a no keyword.

In the following area virtual-link command, the no keyword is optional, This means that the entire syntax can be negated. Depending on the command or the parameters, command negation can mean the disabling of one entire feature for the router or the disabling of that feature for a specific ID, interface or address.

```
(no) area AREAADDRESSID virtual-link ROUTERID(AUTHENTICATE|MSGD|INTERVAL)
```

In the following example, negation is for the base command only. The negated form does not take any parameter.

```
        default-metric <1-16777214>
    no default-metric
```

1.3.3 Variable Parameter Expansion

For the area virtual-link command,

`(no) area AREAADDRESSID virtual-link ROUTERID(AUTHENTICATE|MSGD|INTERVAL)`

the AREAADDRESSID parameter is replaced by either an IP address or a number in the given range:

`AREAADDRESSID=A.B.C.D|<0-4294967295>`

and ROUTERID by an IP address. The minimum command then is:

```
area 10.10.0.11 virtual-link 10.10.0.12
```

The parameters in the string (AUTHENTICATE|MSGD|INTERVAL) are optional, and only one may be chosen. Each one can be replaced by more keywords and parameters. One of these parameters, MD5, is replaced by the following string:

```
MD5= [message-digest-key <1-255> md5 MD5_KEY]
```

with MD5_KEY replaced by a 1-16 character string.

1.4 Show Command Tokens

Two tokens modify the output of the show commands. Use the ? after typing the command to display:

```
# show users
    |  Output modifiers
    >  Output redirection
```

These tokens are available only through the IMI shell; they are unavailable to users who telnet to daemons.

1.4.1 Output Modifiers

Type the | (vertical bar) to use Output modifiers.

```
begin     Begin with the line that matches
exclude   Exclude lines that match
include   Include lines that match
redirect  Redirect output
```

1.4.1.1 Begin

The begin parameter displays the output beginning with the first line containing a token matching the input string (everything typed after the `begin` token).

```
# show run | begin eth1
   ...skipping
   interface eth1
    ipv6 address fe80::204:75ff:fee6:5393/64
   !
   interface eth2
    ipv6 address fe80::20d:56ff:fe96:725a/64
   !
   line con 0
    login
   line vty 0 4
    login
   !
   end
```

1.4.1.2 Exclude

The exclude parameter excludes all lines of output that contain the input string. In the following output all lines containing the word “include” are excluded:

```
# show interface eth1 | exclude input
   Interface eth1
     Scope: both
     Hardware is Ethernet, address is 0004.75e6.5393
     index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
     VRF Binding: Not bound
     Label switching is disabled
     No Virtual Circuit configured
     Administrative Group(s): None
     DSTE Bandwidth Constraint Mode is MAM
     inet6 fe80::204:75ff:fee6:5393/64
     output packets 4438, bytes 394940, dropped 0
     output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
     collisions 0
```

1.4.1.3 Include

The include parameter includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface eth1 | include input
   input packets 80434552, bytes 2147483647, dropped 0, multicast packets
   0
   input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

1.4.1.4 Redirect

The redirect parameter puts the lines of output into the indicated file.

```
# show history | redirect /var/frame.txt
```

1.4.2 Output Redirection

The output redirection token > allows the user to specify a target file for the lines of output.

```
# show history > /var/frame.txt
```

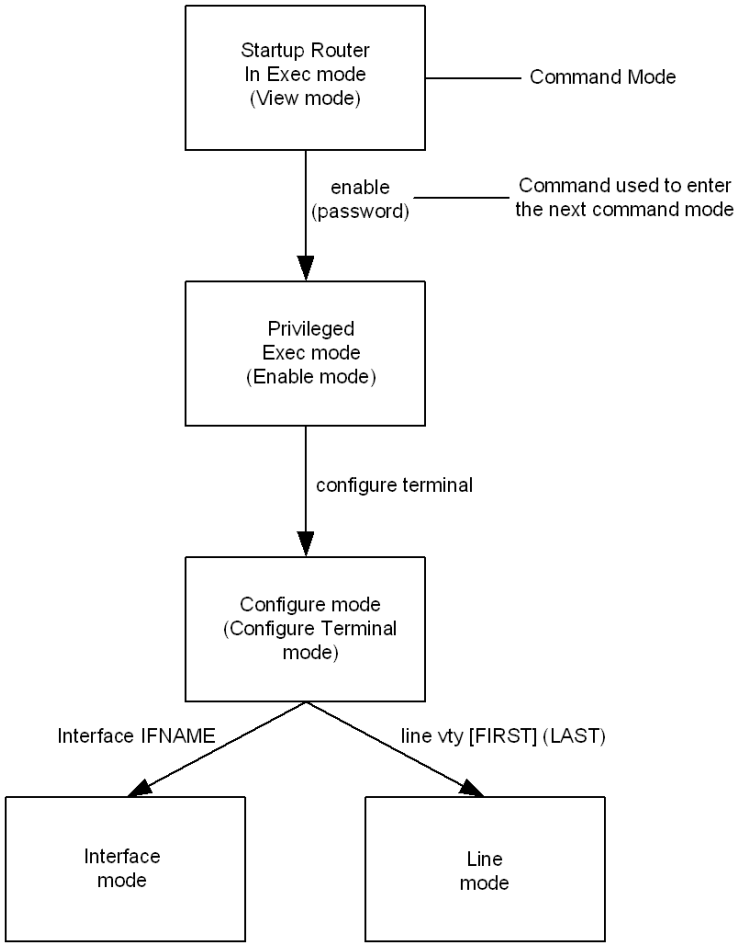
1.5 Common Command Modes

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

Multiple users can telnet and issue commands using the Exec mode and the Privileged Exec mode.

This diagram displays the common command mode tree.

Figure 1-1 Common Command Mode Tree



1.6 Command Common to Multiple Protocols

Refer the to this manual, *SRstackware Intelligent Network Software Layer 3 Command Reference*, and the *SRstackware Intelligent Network Software Switch Configuration Command Reference* for information about using these commands in multiple protocol daemons.

Command Name	Use this Command to
access-class	filter a connection based on an IP access list, for IPv4 networks
access-list	configure an access-list for filtering packets.
access-list extended	configure an extended access-list for filtering packets.
access-list standard	configure a standard access-list for filtering packets.
banner	toggle the displaying of the banner text.
clear ip prefix-list	clear the IP prefix-list.
configure terminal	enter the Configure Terminal mode.
copy running-config startup-config	copy the current running configuration to the startup configuration file.
description	provide interface-specific information.
disable	exit Privileged Exec mode.
enable	enter the Privileged Exec mode.
enable password	change the password for the enable command.
end	leave the current mode.
exec-timeout	set command interpreter wait interval.
exit	leave the current mode, or logout of the session.
help	display online text assistance.
hostname	set or change network server name.
ip prefix-list	create an entry for a prefix list.
ipv6 access-class	filter connection based on an IP access list for IPv6 networks.
ipv6 access-list	configure an access-list for filtering frames.
ipv6 prefix-list	create an entry for an IPv6 prefix list.
line vty	enter Line mode.

Command Name	Use this Command to
list	list all commands for a mode.
log file	specify the file that collects logging information.
log record-priority	specify the logging of the priority of a message.
log syslog	begin logging information to the system log.
log trap	limit logging to a specified level or type.
login	set a password prompt and enable password checking.
match as-path	match an autonomous system path access list.
match community	specify the community to be matched.
match extcommunity	specify the extended community to be matched.
match interface	define the interface match criterion.
match ip address	specify the match address of route.
match ip address prefix-list	specify to match entries of prefix-lists.
match ip next-hop	specify a next-hop address to be matched in a route-map.
match ip next-hop prefix-list	specify the next-hop IP address match criterion, using the prefix-list.
match ipv6 address	specify the match IPv6 address of route.
match ipv6 address prefix-list	match entries of IPv6 prefix-lists.
match ipv6 next-hop	specify a next-hop IPv6 address to be matched by the route-map.
match metric	match a metric of a route.
match origin	match origin code.
match route-type	match specified external route type.
match tag	match the specified tag value.
password	specify a network password.
quit	leave the current mode.
route-map	enter the route-map mode and to permit or deny match/set operations.
service advanced-vty	set the VTY session to Privileged Exec mode instead of the Exec mode (which is the default).

Command Name	Use this Command to
service password-encryption	specify encryption of passwords.
service terminal-length	set the terminal length for VTY sessions.
set aggregator	set the AS number for the route map and router ID.
set as-path	modify an autonomous system path for a route.
set atomic-aggregate	set an atomic aggregate attribute.
set comm-list delete	delete matching communities from inbound or outbound updates.
set community	set the communities attribute.
set community-additive	add a community to the already existing communities.
set dampening	set route-flap dampening parameters.
set extcommunity	set an extended community attribute.
set ip next-hop	set the specified next-hop value.
set ipv6 next-hop	set a next hop-address.
set metric	set a metric value for a route.
set metric-type	set the metric type for the destination routing protocol.
set next-hop	specify the next-hop address.
set origin	set the origin code.
set originator-id	set the originator ID attribute.
set tag	set specified tag value.
set vpnv4 next-hop	set a VPNv4 next-hop address.
set weight	set weights for the routing table.
show access-list	display the list of IP access lists.
show cli	display the CLI tree of the current mode.
show list	display a list of all commands in the current mode.
show history	display all commands used in a session.
show ip prefix-list	display the prefix list entries.
show memory all	display the memory reports for all protocols.

Command Name	Use this Command to
show memory free	display the statistics of free memory for all protocol.
show memory summary	display the summary of memory subsystem statistics.
show route-map	display user readable route-map information.
show running-config	display the current configuration.
show startup-config	display the startup configuration (from storage).
show version	display the current SRstackware version.
terminal length	set the number of lines in a terminal display.
terminal monitor	display debugging on a monitor.
who	display other VTY connections.
write file and write memory	write the current configuration file.
write terminal	display current configurations to the VTY terminal.

Spanning Tree Protocol Commands

2.1 Introduction

This chapter lists the commands that are exclusive to the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

2.2 bridge cisco-interoperability

Use this command to enable/disable Cisco interoperability for the Multiple Spanning Tree Protocol (MSTP).

2.2.1 Command Syntax

`bridge <1-32> cisco-interoperability (enable|disable)`

`<1-32>` Specify the bridge group ID.

`enable` Enable Cisco interoperability for MSTP bridge.

`disable` Disable Cisco interoperability for MSTP bridge

2.2.2 Default

If this command is not used, Cisco interoperability is disabled.

2.2.3 Command Mode

Configure mode

2.2.4 Usage

If Cisco interoperability is required, all SRstackware boxes in the switched LAN must be Cisco-interoperability enabled. When SRstackware is interoperating with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN to instance mapping is not used to classify regions when interoperating with Cisco.

2.2.5 Examples

To enable Cisco interoperability on a Layer 2 switch for a particular bridge (bridge 2 in this example):

```
# configure terminal
(config)# bridge 2 cisco-interoperability enable
```

To disable Cisco interoperability on a Layer 2 switch for a particular bridge:

```
# configure terminal
(config)# bridge 2 cisco-interoperability disable
```

2.3 bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances. To restore the default value of 15 seconds, use the no parameter with this command.

2.3.1 Command Syntax

`bridge <1-32> forward-time FORWARD_DELAY`

`no bridge <1-32> forward-time`

`<1-32>` The ID of the bridge group to which this delay time is assigned.

`FORWARD_DELAY = <4-30>` The forwarding time delay in seconds.

2.3.2 Command Mode

Configure mode

2.3.3 Default

The default value is 15 seconds.

2.3.4 Usage

The allowable range for forward-time is 4-30 seconds. Care should be exercised if the value is to be made below 7 seconds.

2.3.5 Example

```
# configure terminal
(config)# bridge 3 forward-time 6
```

2.3.6 Related Commands

bridge protocol ieee

2.4 bridge hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change.

This value is used by all instances. To restore the default value of the hello time, use the no parameter.

2.4.1 Command Syntax

`bridge <1-32> hello-time HELLOTIME`

`no bridge <1-32> hello-time`

`<1-32>` The ID of the bridge group to which this hello time is assigned.

`HELLOTIME = <1-10>` The hello BPDU interval in seconds.

2.4.2 Command Mode

Configure mode

2.4.3 Default

Default value is 2 seconds.

2.4.4 Usage

Configure the bridge instance name before using this command. The allowable range of values is 1-10 seconds. However, make sure that the value of hello time is always greater than the value of hold time (1 second by default).

2.4.5 Example

```
# configure terminal
(config)# bridge 3 hello-time 3
```

2.5 bridge instance priority

Set the bridge priority for an MST instance to the value specified.

To restore the default value of the bridge priority, use the no parameter with this command.

2.5.1 Command Syntax

`bridge <1-32> instance INSTANCE_ID priority BRIDGE_PRIORITY`

`no bridge <1-32> instance INSTANCE_ID priority`

`<1-32>` Specify the bridge-group ID.

`INSTANCE_ID` Specify the instance ID in the range of <1-64>.

`BRIDGE_PRIORITY <0-61440>` Specify the bridge priority (a lower priority indicates a greater likelihood of the bridge becoming root).

2.5.2 Command Mode

Configure mode.

2.5.3 Default

The default value of the priority for each instance is 32768.

2.5.4 Usage

The lower the priority of the bridge, the better the chances are of the bridge becoming a root bridge or a designated bridge for the LAN.

The permitted range of values is 0-61440. The priority values can be set only in increments of 4096.

2.5.5 Examples

```
# configure terminal
(config)# bridge 4 instance 3 priority 0
(config)# no bridge 4 instance 3 priority
```

2.6 bridge instance vlan

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge. This command can be used only after the VLANs are defined.

Use the no parameter with this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

2.6.1 Command Syntax

`bridge <1-32> instance INSTANCE_ID vlan VLAN_ID`

`no bridge <1-32> vlan VLAN_ID`

`<1-32>` Specify the bridge-group ID.

`INSTANCE_ID` Specify the instance ID in the range of <1-64>.

`VLAN_ID` Specify multiple VLAN IDs corresponding to the bridge instance, for example, `vlan 10,11 or vlan 10-15.` The range of valid values is `<1-4022>.`

2.6.2 Command Mode

Spanning-Tree MST Configuration Mode

2.6.3 Usage

The permitted range of instances is 0-64. Instance 0 refers to the internal spanning tree. The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

2.6.4 Examples

To associate multiple VLANs, in this case VLANs 10 and 20 to instance 1 of bridge 1:

```
# configure terminal
(config)# bridge 1 protocol mstp
(config)# spanning-tree mst configuration
(config-mst)# bridge 1 instance 1 vlan 10,20
```

To associate multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 to instance 1 of bridge 1:

```
# configure terminal
(config)# bridge 1 protocol mstp
(config)# spanning-tree mst configuration
(config-mst)# bridge 1 instance 1 vlan 10-15
```

To delete multiple VLANs, in this case, VLANs 10 and 11 from instance 1 of bridge 1:

```
# configure terminal
(config)# bridge 1 protocol mstp
(config)# spanning-tree mst configuration
(config-mst)# no bridge 1 instance 1 vlan 10,11
```

To delete multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 from instance 1 of bridge 1:

```
# configure terminal
(config)# bridge 1 protocol mstp
(config)# spanning-tree mst configuration
(config-mst)# no bridge 1 instance 1 vlan 10-15
```

2.7 bridge max-age

Use this command to set the maximum age for a bridge. This value is used by all instances. Use the no parameter with this command to restore the default value of the maximum age.

2.7.1 Command Syntax

`bridge <1-32> max-age MAXAGE`

`no bridge <1-32> max-age`

`<1-32>` The ID of the bridge group to which this maximum age time is assigned.

`MAXAGE = <6-40>` The maximum time, in seconds, to listen for the root bridge.

2.7.2 Command Mode

Configure mode

2.7.3 Default

The default value of bridge maximum age is 20 seconds.

2.7.4 Usage

Maximum age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely.

The value of maximum age should be greater than twice the value of hello time plus 1, but less than twice the value of forward delay minus 1. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

2.7.5 Examples

```
# configure terminal
(config)# bridge 2 max-age 12
```

2.8 bridge max-hops

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. To restore the default value, use the no parameter with this command.

2.8.1 Command Syntax

`bridge <1-32> max-hops HOP_COUNT`

`no bridge <1-32> max-hops`

`<1-32>` Specify the bridge-group ID.

`HOP_COUNT` Maximum hops for which the BPDU will be valid.

2.8.2 Command Mode

Configure mode

2.8.3 Default

The default maximum hops in an MST region are 20.

2.8.4 Usage

Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU.

2.8.5 Examples

```
# configure terminal
(config)# bridge 3 max-hops 25
```

2.9 bridge multiple-spanning-tree enable

Use this command to enable MSTP on a bridge. Use the no parameter to disable maximum on the bridge.

2.9.1 Command Syntax

`bridge <1-32> multiple-spanning-tree enable`

`no bridge <1-32> multiple-spanning-tree enable (bridge-forward)`

`<1-32>` Bridge-group ID used for bridging.

`bridge-forward` (Optional) Puts all ports of the specified bridge into forwarding state.

2.9.2 Command Mode

Configure mode

2.9.3 Default

If the bridge-forward option is not entered when using the no parameter, the default behavior is to put all bridge ports in blocking state.

2.9.4 Examples

```
# configure terminal
(config)# bridge 2 multiple-spanning-tree enable
# configure terminal
(config)# no bridge 2 multiple-spanning-tree enable bridge-forward
```

2.10 bridge priority

Use this command to set the bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root.

Use the no form of the command to reset it to the default value.

2.10.1 Command Syntax

`bridge <1-32> priority PRIORITY`

`no bridge <1-32> priority`

`<1-32> =` The ID of the bridge group for which the priority is set.

`PRIORITY = <0-61440>` The bridge priority.

2.10.2 Command Mode

Configure mode

2.10.3 Default

The default priority is 32678 (or hex 0x8000).

2.10.4 Usage

This command must be used to set the priority of the bridge. The priority values can be set only in increments of 4096.

2.10.5 Examples

```
# configure terminal
(config)# bridge 2 priority 4096
```

2.11 bridge rapid-spanning-tree enable

Use this command to enable the Rapid Spanning Tree Protocol (RSTP) on a bridge. Use the no form of the command to disable the Rapid Spanning Tree protocol on a bridge.

2.11.1 Command Syntax

`bridge <1-32> rapid-spanning-tree enable`

`no bridge <1-32> rapid-spanning-tree enable bridge-forward`

`<1-32>` Bridge group name used for bridging.

`bridge-forward` Puts all ports of the specified bridge into the forwarding state.

2.11.2 Command Mode

Configure mode

2.11.3 Default

When the `bridge-forward` option is not used with the `no` parameter, the default behavior puts all bridge ports in the blocking state.

2.11.4 Usage

Use this command to enable or disable RSTP on a specific bridge. Use the `bridge-forward` option with the `no` form of the command to place all ports on the specified bridge into the forwarding state.

2.11.5 Examples

```
# configure terminal
(config)# bridge 2 rapid-spanning-tree enable
# configure terminal
(config)# no bridge 2 rapid-spanning-tree enable bridge-forward
```

2.12 bridge region

Use this command to create an MST region, and specify a name to it. MST bridges of a region form different spanning trees for different VLANs.

2.12.1 Command Syntax

`bridge <1-32> region REGION_NAME`

`no bridge <1-32> region REGION_NAME`

`<1-32>` Specify the bridge-group ID.

`REGION_NAME` Specify the name of the region.

2.12.2 Command Mode

MST Configuration mode

2.12.3 Default

By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

2.12.4 Examples

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# bridge 3 region IPI
```

2.13 bridge revision

Use this command to specify the number for configuration information.

2.13.1 Command Syntax

`bridge <1-32> revision REVISION_NUM`

`<1-32>` Specify the bridge-group ID.

`REVISION_NUM <0-255>` Revision number.

2.13.2 Command Mode

MST Configuration Mode

2.13.3 Default

The default value of revision number is 0.

2.13.4 Examples

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# bridge 3 revision 25
```

2.14 bridge shutdown

Use this command to disable a bridge. Use the no parameter to reset the bridge.

2.14.1 Command Syntax

`bridge shutdown <1-32>`

`no bridge shutdown <1-32>`

`<1-32>` Bridge-group ID used for bridging.

2.14.2 Command Mode

Configure mode

2.14.3 Usage

Make sure to use the `bridge instance NAME` command before using this command.

2.14.4 Examples

```
# configure terminal
(config)# bridge shutdown 4
```

2.14.5 Related Commands

bridge instance

2.15 bridge spanning-tree enable

Use this command to enable the Spanning Tree Protocol on a bridge. Use the no parameter to disable the Spanning Tree Protocol on the bridge.

2.15.1 Command Syntax

`bridge <1-32> spanning-tree enable`

`no bridge <1-32> spanning-tree enable (bridge-forward)`

`<1-32>` Bridge-group ID used for bridging.

`bridge-forward` (Optional) Puts all ports of the specified bridge into forwarding state.

2.15.2 Command Mode

Configure mode

2.15.3 Default

If the bridge-forward option is not entered when using the no parameter, the default behavior is to put all bridge ports in blocking state.

2.15.4 Examples

```
# configure terminal
(config)# bridge 2 spanning-tree enable
# configure terminal
(config)# no bridge 2 spanning-tree enable bridge-forward
```

2.16 bridge spanning-tree errdisable-timeout enable

Use this command to enable the error-disable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

2.16.1 Command Syntax

`bridge <1-32> spanning-tree errdisable-timeout enable`

`<1-32>` Bridge group name for bridging.

2.16.2 Command Mode

Configure mode

2.16.3 Default

By default, the port is enabled after 300 seconds.

2.16.4 Usage

The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port gets enabled back without manual intervention after a set interval. This interval can be configured by using the `bridge spanning-tree errdisable-timeout interval` command.

2.16.5 Examples

```
# configure terminal
(config)# bridge 1 spanning-tree errdisable-timeout enable
```

2.17 bridge spanning-tree errdisable-timeout interval

Use this command to specify the time interval after which a port is brought back up.

2.17.1 Command Syntax

`bridge <1-32> spanning-tree errdisable-timeout interval <10-1000000>`

`<1-32>` Bridge group name for bridging.

`<10-1000000>` Specify the error-disable-timeout interval in seconds.

2.17.2 Command Mode

Configure mode

2.17.3 Default

By default, the port is enabled after 300 seconds.

2.17.4 Examples

```
# configure terminal
(config)# bridge 4 spanning-tree errdisable-timeout interval 34
```

2.18 bridge spanning-tree pathcost

Use this command to set a spanning-tree path cost method.

Use the no option with this command to return the path cost method to the default setting.

2.18.1 Command Syntax

`bridge <1-32> spanning-tree pathcost method [long|short]`

`no bridge <1-32> spanning-tree pathcost method`

`<1-32>` ID of the bridge group

`method` Method used to calculate default port path cost

`long` Use 16-bit based values for default port path costs

`short` Use 32-bit based values for default port path costs

2.18.2 Command Mode

Configure mode

2.18.3 Default

The default path cost method for STP is short and for MSTP/RSTP is long.

2.18.4 Usage

If the short method is chosen, the switch uses a value for the default path cost a number in the range 1 through 65,535. If the long method is chosen, the switch uses a value for the default path cost a number in the range 1 through 200,000,000.

Use the `show bridge <1-32> spanning-tree pathcost method` command to display administratively configured and current running pathcost method running on the bridge.

2.18.5 Example

```
# configure terminal
(config)# bridge 1 spanning-tree pathcost method short
```

2.19 bridge spanning-tree portfast bpdu-filter

Use this command to set the portfast BPDU filter for the bridge. All ports that have their BPDU filter set to default take the same value of BPDU filter as that of the bridge.

Use the no parameter with this command to disable the BPDU filter for the bridge.

2.19.1 Command Syntax

`(no) bridge <1-32> spanning-tree portfast bpdu-filter`

<1-32> Bridge group name for bridging.

2.19.2 Command Mode

Configure mode

2.19.3 Usage

The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures that PortFast-enabled ports do not transmit or receive any BPDUs.

Use the show spanning tree command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port.

2.19.4 Examples

```
# configure terminal
(config)# bridge 3 spanning-tree portfast bpdu-filter
```

2.19.5 Related Commands

`spanning-tree portfast bpdu-filter`

2.20 bridge spanning-tree portfast bpdu-guard

Use this command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge.

Use the no parameter with this command to disable the BPDU Guard feature on a bridge.

2.20.1 Command Syntax

`(no) bridge <1-32> spanning-tree portfast bpdu-guard`

<1-32> Bridge group name for bridging.

2.20.2 Command Mode

Configure mode

2.20.3 Usage

When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have the BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. You can either bring the port back up manually by using the no shutdown command, or configure the errdisable-timeout feature to enable the port after the specified time interval.

Use the show spanning-tree command to display the bridge and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of BPDU guard.

2.20.4 Examples

```
# configure terminal
(config)# bridge 1 spanning-tree portfast bpdu-guard
```

2.20.5 Related Commands

`spanning-tree portfast bpdu-guard`, **`show spanning-tree`**

2.21 bridge transmit-holdcount

Use this command to set the maximum number of transmissions of BPDUs by the transmit state machine.

Use the no parameter with this command to restore the default transmit hold-count value.

2.21.1 Command Syntax

`(no) bridge <1-32> transmit-holdcount <1-10>`

`<1-32>` The ID of the bridge group to which this transmit hold-count is assigned.

`<1-10>` Transmit hold-count value.

2.21.2 Command Mode

Configure mode

2.21.3 Default

Transmit hold-count default value is 3.

2.21.4 Examples

```
# configure terminal
(config) # bridge 1 transmit-holdcount 5
```

2.22 bridge-group instance

Use this command to assign a Multiple Spanning Tree (MST) instance to a port.

Use the no parameter with this command to remove the instance.

2.22.1 Command Syntax

`bridge-group <1-32> instance INSTANCE_ID`

`no bridge-group <1-32> instance`

`<1-32>` Specify the bridge-group number for bridging.

`INSTANCE_ID` Specify the instance ID in the range of <1-64>

2.22.2 Command Mode

Interface mode

2.22.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# bridge-group 4 instance 3
```

2.23 bridge-group instance path-cost

Use this command to set the cost of a path associated with an interface.

Use the no parameter with this command to restore the default cost value of the path.

2.23.1 Command Syntax

`bridge-group <1-32> instance INSTANCE_ID path-cost <1-200000000>`

`no bridge-group <1-32> path-cost`

`<1-32>` The bridge-group number for bridging

`INSTANCE_ID` The instance ID in the range of <1-64>

`path-cost <1-200000000>` Specify the cost of path in the range of <1-200000000> (a lower path-cost indicates a greater likelihood of the specific interface becoming a root).

2.23.2 Command Mode

Interface mode

2.23.3 Default

Assuming a 10 Mb/s link speed, the default value is configured as 200,000.

2.23.4 Usage

Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the bridge-group instance command (see the example below).

2.23.5 Examples

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)# bridge 4 instance 3 vlan 3
(config-mst)# exit
(config)# interface eth1
(config-if)# bridge-group 4 instance 3
```

```
(config-if)# bridge-group 4 instance 3 path-cost 1000
```

2.23.6 Related Commands

`bridge instance vlan, bridge-group instance`

2.24 bridge-group instance priority

Use this command to set the port priority for a bridge group.

Use the no parameter with this command to restore the default priority value.

2.24.1 Command Syntax

`bridge-group <1-32> instance INSTANCE_ID priority PRIORITY`

`no bridge-group <1-32> instance INSTANCE_ID`

`<1-32>` The bridge-group number for bridging

`INSTANCE_ID` Specify the instance ID in the range of <1-64>

`PRIORITY <0-240>` Specify the port priority in a range of <0-240> (a lower priority indicates greater likelihood of the interface becoming a root).

2.24.2 Command Mode

Interface mode

2.24.3 Default

The default value of port priority for each instance is 128.

2.24.4 Usage

The Multiple Spanning Tree Protocol 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 a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

The permitted range is 0-240. The priority values can only be set in increments of 16.

2.24.5 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# bridge-group 4 instance 3 priority 121
```

2.25 bridge-group path-cost

Use this command to set the cost of a path associated with a bridge group. The lower the path cost, the greater the likelihood of the bridge becoming root.

2.25.1 Command Syntax

`bridge-group <1-32> path-cost PATHCOST`

`no bridge-group <1-32> path-cost`

`<1-32>` the ID of the bridge group.

`PATHCOST = <1-200000000>` The cost to be assigned to the group.

2.25.2 Command Mode

Interface mode

2.25.3 Default

The default bridge-group path cost is 0.

2.25.4 Examples

```
# configure terminal
(config)# interface eth1
(config-if)# bridge-group 3 path-cost 123
```

2.26 bridge-group priority

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

2.26.1 Command Syntax

`bridge-group <1-32> priority PRIORITY`

`<1-32>` the ID of the bridge group.

`PRIORITY = <0-240>` The priority, in increments of 16, to be assigned to the group.

2.26.2 Command Mode

Interface mode

2.26.3 Default

The default priority is 1.

2.26.4 Examples

```
# configure terminal
(config)# interface eth1
(config-if)# bridge-group 4 priority 96
```

2.27 clear spanning-tree detected protocols

Use this command to clear the detected protocols for a specific bridge or interface.

2.27.1 Command Syntax

`clear spanning-tree detected protocols [bridge <1-32>]|[interface IFNAME]`

`<1-32>` Specify the number of the bridge group on which protocols have to be cleared.

`IFNAME` Specify the name of the interface on which protocols have to be cleared

2.27.2 Command Mode

Privileged Exec mode

2.27.3 Usage

This command begins the port migration as per IEEE 802.1w-2001, Section 17.26.

After issuing this command, the migration timer is started on the port, only if the force version is RSTP or MSTP (greater versions of RSTP).

2.27.4 Examples

```
# clear spanning-tree detected protocols bridge 2
```

2.28 debug mstp

Use this command to turn on, and turn off, debugging and echoing data to the console, at various levels.

NOTE: This command enables MSTP, RSTP, and STP debugging.

Use the no parameter with this command to turn off debugging.

2.28.1 Command Syntax

`debug mstp (all|cli|PACKET|PROTOCOL|TIMER)`

`all` echoes all Spanning-tree debugging levels to the console.

`cli` echoes Spanning-tree commands to the console.

`PACKET = packet rx|tx` echoes Spanning-tree packets to the console.

`rx` received packets.

`tx` transmitted packets.

`PROTOCOL` protocol (detail) echoes protocol changes to the console.

`TIMER` timer (detail) echoes timer start to the console.

`detail` detailed output.

2.28.2 Command Mode

Exec, Privileged Exec, and Configure modes

2.28.3 Examples

```
# configure terminal
(config)# debug mstp all
(config)# debug mstp cli
(config)# debug mstp packet rx
(config)# debug mstp protocol detail
(config)# debug mstp timer
```

2.29 show bridge spanning-tree pathcost

Use this command to display the administratively-configured and currently-running path cost method for the bridge.

2.29.1 Command Syntax

```
show bridge <1-32> spanning-tree pathcost method
```

<1-32> ID of the bridge group

2.29.2 Command Mode

Exec mode

2.29.3 Usage

The following is sample output from this command that displays the path cost method:

```
% Spanning tree default pathcost method used is long
```

2.29.4 Example

ZebOS# show bridge 2 spanning-tree pathcost method

2.30 show debugging mstp

Use this command to display the status of the debugging of the MSTP system.

2.30.1 Command Syntax

```
show debugging mstp
```

2.30.2 Command Mode

Exec and Privileged Exec mode

2.30.3 Examples

```
# show debugging mstp
```

2.31 show spanning-tree

Use this command to show the state of the spanning tree for all named bridge groups.

2.31.1 Command Syntax

```
show spanning-tree
```

2.31.2 Command Mode

Privileged Exec, Configure, and Interface modes

2.31.3 Usage

The following is an output of this command displaying the spanning tree information for bridge 1, eth2, eth1 and Default.

```
# show spanning-tree
% 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 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
```

```
% 1: portfast errdisable timeout interval 300 sec
% eth2: Ifindex 5 - Port Id 8005 - Role Designated - State Forwarding
% eth2: Designated Path Cost 0
% eth2: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth2: Designated Port Id 8005 - Priority 128 -
% eth2: Root 80000002b328530a
% eth2: Designated Bridge 80000002b328530a
% eth2: Message Age 0 - Max Age 20
% eth2: Hello Time 2 - Forward Delay 15
% eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% eth2: forward-transitions 4
% eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% eth2: No portfast configured - Current portfast off
% eth2: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth2: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth2: no root guard configured- Current root guard off
% eth2: Configured Link Type point-to-point - Current point-to-point
%
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
```

```
%%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Thu Jan 1 05:30:00 1970
% 0: 0 topology change(s) - last topology change Thu Jan 1
% Default: portfast bpdu-filter disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
```

2.31.4 Examples

```
# show spanning-tree
```

2.32 show spanning-tree interface

Use this command to show the state of the spanning tree for all named STP or RSTP bridge-groups of the specified interface

NOTE: To show the state of the spanning tree for MSTP bridge-groups, use the show spanning-tree mst interface command.

2.32.1 Command Syntax

```
show spanning-tree interface IFNAME
```

2.32.2 Command Mode

Enable mode

2.32.3 Examples

The following is an output of this command displaying the state of the spanning tree of the interface eth0.

```
# show spanning-tree interface eth0
% 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 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
% eth1: Configured Link Type point-to-point - Current point-to-point
```

2.33 show spanning-tree mst

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it.

2.33.1 Command Syntax

```
show spanning-tree mst
```

2.33.2 Command Mode

Enable mode and Interface mode

2.33.3 Usage

The following is an output of this command displaying the number of instances created, and the VLANs associated with it.

```
# show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec %
% Instance VLAN
% 0: 1
% 2: 3-4
% 2: 3-4
```

2.34 show spanning-tree mst config

Use this command to display MSTP configuration information for a bridge.

2.34.1 Command Syntax

```
show spanning-tree mst config
```

2.34.2 Command Mode

Enable mode and Interface mode

2.34.3 Usage

The following show output displays the MSTP configuration information for bridge b.

```
# show spanning-tree mst config
%
%  MSTP Configuration Information for bridge b :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0x80DEE46DA92A98CF21C603291B22880A
%-------------------------------------------------------
```

2.35 show spanning-tree mst detail

Use this command to display detailed information about each instance, and all interfaces associated with that particular instance.

2.35.1 Command Syntax

```
show spanning-tree mst detail
```

2.35.2 Command Mode

Enable mode and Interface mode

2.35.3 Usage

The following is an output of this command displaying detailed information about each instance, and all interfaces associated with them.

```
# show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 0
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 0000009027342b72
% 1: CIST Reg Root Id 0000009027342b72
% 1: CST Bridge Id 0000009027342b72
```

```
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%   eth2: Port 4 - Id 8004 - Role Designated - State Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth2: Designated Port Id 8004 - CST Priority 128  -
%   eth2: CIST Root 0000009027342b72
%   eth2: Regional Root 0000009027342b72
%   eth2: Designated Bridge 0000009027342b72
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   eth2: Version Multiple Spanning Tree Protocol - Received None - Send
STP
%   eth2: No portfast configured - Current  portfast off
%   eth2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   eth2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%
%   eth1: Port 3 - Id 8003 - Role Designated - State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 8003 - CST Priority 128  -
%   eth1: CIST Root 0000009027342b72
%   eth1: Regional Root 0000009027342b72
%   eth1: Designated Bridge 0000009027342b72
%   eth1: Message Age 0 - Max Age 20
%   eth1: CIST Hello Time 2 - Forward Delay 15
%   eth1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   eth1: Version Multiple Spanning Tree Protocol - Received STP - Send STP
%   eth1: No portfast configured - Current  portfast off
%   eth1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   eth1: portfast bpdu-filter default  - Current portfast bpdu-filter off
```

```
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%
% Instance  1:  Vlans: 2
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8001009027342b72
% 1: MSTI Bridge Id 8001009027342b72
%   eth2: Port 4 - Id 8004 - Role Designated - State Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8001009027342b72
%   eth2: Designated Bridge 8001009027342b72
%   eth2: Message Age 0 - Max Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
%   eth1: Port 3 - Id 8003 - Role Designated - State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured CST External Path cost 200000
%   eth1: CST Priority 128  - MSTI Priority 128
%   eth1: Designated Root 8001009027342b72
%   eth1: Designated Bridge 8001009027342b72
%   eth1: Message Age 0 - Max Age 0
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

2.36 show spanning-tree mst detail interface

Use this command to display the filtering database values. This command prints the detailed information about each instance, and the specified interface associated with that particular instance.

2.36.1 Command Syntax

```
show spanning-tree mst detail interface IFNAME
```

2.36.2 Command Mode

Enable mode

2.36.3 Examples

The following is an output of this command displaying detailed information about each instance, and the interface eth1 associated with them.

```
# show spanning-tree mst detail interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated – State Forwarding
% eth1: Designated External Path Cost 0 -Internal Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 2
% eth1: Designated Port Id 8004 - CIST Priority 128 -
% eth1: CIST Root 80000002b328530a
% eth1: Regional Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: CIST Hello Time 2 - Forward Delay 15
% eth1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo
change timer 0
% eth1: forward-transitions 1
% eth1: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
```

```
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
% eth1: Configured Link Type point-to-point – Current point-to-point
%
% Instance 2: Vlans: 3-4
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020002b328530a
% 1: MSTI Bridge Id 80020002b328530a
% eth1: Ifindex 4 - Port Id 8004 - Role Designated – State Forwarding
% eth1: Designated Internal Path Cost 0 - Designated Port Id 8004
% eth1: Configured Internal Path Cost 200000
% eth1: Configured CST External Path cost 200000
% eth1: CST Priority 128 - MSTI Priority 128
% eth1: Designated Root 80020002b328530a
% eth1: Designated Bridge 80020002b328530a
% eth1: Message Age 0 - Max Age 0
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

2.37 show spanning-tree mst instance

Use this command to display detailed information for the specified instance, and all interfaces associated with that instance.

2.37.1 Command Syntax

`show spanning-tree mst instance INSTANCE_ID`

`INSTANCE_ID` Specify the instance ID, in the range of <1-64>, for which information needs to be displayed.

2.37.2 Command Mode

Enable mode and Interface mode

2.37.3 Usage

The following is an output of this command displaying detailed information for instance 2.

```
# show spanning-tree mst instance 2
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020002b328530a
% 1: MSTI Bridge Id 80020002b328530a
% eth2: Ifindex 5 - Port Id 8005 - Role Designated – State Forwarding
% eth2: Designated Internal Path Cost 0 - Designated Port Id 8005
% eth2: Configured Internal Path Cost 200000
% eth2: Configured CST External Path cost 200000
% eth2: CST Priority 128 - MSTI Priority 128
% eth2: Designated Root 80020002b328530a
% eth2: Designated Bridge 80020002b328530a
% eth2: Message Age 0 - Max Age 0
% eth2: Hello Time 2 - Forward Delay 15
% eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%
% eth1: Ifindex 4 - Port Id 8004 - Role Designated – State Forwarding
% eth1: Designated Internal Path Cost 0 - Designated Port Id 8004
% eth1: Configured Internal Path Cost 200000
% eth1: Configured CST External Path cost 200000
% eth1: CST Priority 128 - MSTI Priority 128
% eth1: Designated Root 80020002b328530a
% eth1: Designated Bridge 80020002b328530a
% eth1: Message Age 0 - Max Age 0
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%%
% bridge 0 is not configured as MSTP bridge
```

2.38 show spanning-tree mst instance interface

Use this command to display detailed information for the specified instance, and the specified interface associated with that instance.

2.38.1 Command Syntax

```
show spanning-tree mst instance <1-15> interface IFNAME
```

2.38.2 Command Mode

Enable mode

2.38.3 Example

The following is an output of this command displaying detailed information for instance 1 & interface eth1.

```
# show spanning-tree mst instance 1 interface eth1
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020002b328530a
% 1: MSTI Bridge Id 80020002b328530a
% eth1: Ifindex 4 - Port Id 8004 - Role Designated – State Forwarding
% eth1: Designated Internal Path Cost 0 - Designated Port Id 8004
% eth1: Configured Internal Path Cost 200000
% eth1: Configured CST External Path cost 200000
% eth1: CST Priority 128 - MSTI Priority 128
% eth1: Designated Root 80020002b328530a
% eth1: Designated Bridge 80020002b328530a
% eth1: Message Age 0 - Max Age 0
% eth1: Hello Time 2 - Forward Delay 15
% eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

2.39 show spanning-tree mst interface

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it for the interface specified.

2.39.1 Command Syntax

```
show spanning-tree mst interface IFNAME
```

2.39.2 Command Mode

Enable mode

2.39.3 Examples

The following is an output of this command displaying detailed information about each instance, and all interfaces associated with them for the interface eth1.

```
# show spanning-tree mst interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000008c73a2b22
% 1: CIST Reg Root Id 80000008c73a2b22
% 1: CST Bridge Id 80000008c73a2b22
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
%   Instance        VLAN
%   0:              1
%   1:              2-3
%   2:              4-5
```

2.40 show traffic-class-table

Use this command to display the data in the traffic class table.

2.40.1 Command Syntax

`show traffic-class-table interface IFNAME`

`IFNAME` Specify the name of the interface.

2.40.2 Command Mode

Privileged Exec mode

2.40.3 Examples

The following is an output of this command displaying the traffic class table for interface eth1.

```
# show traffic-class-table interface eth1
User Prio / Num Traffic Classes
       1  2  3  4  5  6  7  8
   0   0  0  0  0  0  0  0  0
   1   0  0  0  0  0  0  0  0
   2   0  0  0  0  0  0  0  0
   3   0  0  0  0  0  0  0  0
   4   0  0  0  0  0  0  0  0
   5   0  0  0  0  0  0  0  0
   6   0  0  0  0  0  0  0  0
```

2.41 show user-priority

Use this command to display the user priority data.

2.41.1 Command Syntax

```
show user-priority interface IFNAME
```

2.41.2 Command Mode

Privileged Exec mode

2.41.3 Examples

The following is an output of this command displaying set user priority for interface eth4.

```
# show user-priority interface eth4
Default user priority : 7
```

2.42 spanning-tree autoedge

Use this command to assist in automatic identification of the edge port.

Use the no parameter with this command to disable this feature.

2.42.1 Command Syntax

```
(no) spanning-tree autoedge
```

2.42.2 Command Mode

Interface mode

2.42.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree autoedge
```

2.43 spanning-tree edgeport

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

This command is an alias to the spanning-tree portfast command. Both commands can be used interchangeably.

2.43.1 Command Syntax

```
(no) spanning-tree edgeport
```

2.43.2 Command Mode

Interface Mode

2.43.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree edgeport
```

2.44 spanning-tree enable

Use this command to enable the Spanning Tree Protocol (STP) on the default bridge. Use the no parameter with this command to disable the STP on the default bridge.

2.44.1 Command Syntax

`spanning-tree enable`

`no spanning-tree enable (bridge-forward)`

`bridge-forward` Optional. Puts all ports of the default bridge into the forwarding state.

2.44.2 Command Mode

Configure mode

2.44.3 Default

If the bridge-forward option is not entered when using the no parameter, the default is to put all bridge ports in a blocking state.

2.44.4 Examples

```
# configure terminal
(config)# spanning-tree enable
# configure terminal
(config)# no spanning-tree enable bridge-forward
```

2.44.5 Related Commands

`bridge spanning-tree enable`

2.45 spanning-tree force-version

Use this command to specify the version. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-3, for RSTP, the valid range is 0-2.

Use the no parameter with this command to set the default protocol version.

2.45.1 Command Syntax

`(no) spanning-tree force-version VERSION`

`VERSION <0-3>` Version identifier. (0 - STP, 1- Not supported, 2 - RSTP, 3 - MSTP)

2.45.2 Command Mode

Interface mode

2.45.3 Examples

Set the value to enforce the spanning tree protocol:

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree force-version 1
```

Set the default protocol version:

```
# configure terminal
(config)# interface eth0
(config-if)# no spanning-tree force-version
```

2.46 spanning-tree guard root

Use this command to enable the Root Guard feature for the port. This feature disables reception of superior BPDUs.

Use the no parameter with this command to disable the root guard feature for the port.

2.46.1 Command Syntax

(no) spanning-tree guard root

2.46.2 Command Mode

Interface mode

2.46.3 Usage

The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

2.46.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree guard root
```

2.47 spanning-tree hello-time (Interface Mode)

Use this command to configure the hello time of the port for an interface.

Use the no parameter with this command to return to the default value for the hello time.

2.47.1 Command Syntax

```
spanning-tree hello-time <1-10>
no spanning-tree hello-time
```

2.47.2 Command Mode

Interface mode

2.47.3 Default

The default hello-time value is 2.

2.47.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree hello-time 5
```

2.48 spanning-tree instance restricted-role

Use this command to set the restricted role value for the instance to TRUE.

Use the no parameter with this command to set the restricted role value for the instance to FALSE.

2.48.1 Command Syntax

`(no) spanning-tree instance INSTANCE_ID restricted-role`

`INSTANCE_ID` Specify the instance ID in the range of <1-64>.

2.48.2 Command Mode

Interface mode

2.48.3 Default

The default restricted-role value is FALSE.

2.48.4 Example

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree instance 2 restricted-role
```

2.49 spanning-tree instance restricted-tcn

Use this command to set the restricted TCN value for the instance to TRUE.

Use the no parameter with this command to set the restricted TCN value for the instance to FALSE.

2.49.1 Command Syntax

`(no) spanning-tree instance INSTANCE_ID restricted-tcn`

`INSTANCE_ID` Specify the instance ID in the range of <1-64>

2.49.2 Command Mode

Interface mode

2.49.3 Default

The default restricted TCN value is FALSE.

2.49.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree instance 2 restricted-tcn
```

2.50 spanning-tree link-type

Use this command to enable or disable point-to-point or shared link types.

Use the no parameter with this command to disable rapid transition.

2.50.1 Command Syntax

`(no) spanning-tree link-type point-to-point`

`(no) spanning-tree link-type shared`

`shared` Disable rapid transition.

`point-to-point` Enable rapid transition.

2.50.2 Command Mode

Interface mode

2.50.3 Usage

RSTP has a backward-compatible STP mode, spanning-tree link-type shared. An alternative is the spanning-tree force-version 0.

2.50.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree link-type point-to-point
```

2.51 spanning-tree mst configuration

Use this command to enter the Multiple Spanning Tree Configuration mode.

2.51.1 Command Syntax

```
spanning-tree mst configuration
```

2.51.2 Command Mode

Configure mode

2.51.3 Examples

```
# configure terminal
(config)# spanning-tree mst configuration
(config-mst)#
```

2.52 spanning-tree portfast

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

2.52.1 Command Syntax

```
(no) spanning-tree portfast
```

2.52.2 Command Mode

Interface Mode

2.52.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree portfast
```

2.53 spanning-tree portfast bpdu-filter

Use this command to set portfast BPDU filter for the port.

Use the no parameter with this command to revert the port BPDU filter value to default.

2.53.1 Command Syntax

```
(no) spanning-tree portfast bpdu-filter [enable|disable|default]
```

2.53.2 Command Mode

Interface mode

2.53.3 Usage

Use this command to set the BPDU filter value for individual ports. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge level BPDU filter configuration takes effect for the port. Use the bridge spanning-tree portfast bpdu-filter command to configure the BPDU filter feature on a bridge.

Use the show spanning tree command to display administratively configured, and currently running values, of the BPDU filter parameter for the bridge and port.

2.53.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree portfast bpdu-filter enable
```

2.53.5 Related Commands

```
bridge spanning-tree portfast bpdu-filter
```

2.54 spanning-tree portfast bpdu-guard

Use this command to enable or disable the BPDU Guard feature on a port.

Use the no parameter with this command to set the BPDU Guard feature on a port to default.

2.54.1 Command Syntax

`spanning-tree portfast bpdu-guard [enable|disable|default]`

2.54.2 Command Mode

Interface mode

2.54.3 Usage

This command supersedes the bridge level configuration for the BPDU Guard feature. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge-level BPDU Guard configuration takes effect. Use the bridge spanning-tree portfast bpdu-guard command to configure the BPDU Guard feature on a bridge.

Use the show spanning-tree command to display the bridge and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of the BPDU guard.

2.54.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree portfast bpdu-guard enable
```

2.54.5 Related Commands

`bridge spanning-tree portfast bpdu-guard, show spanning-tree`

2.55 spanning-tree restricted-role

Use this command to set the restricted-role value of the port to TRUE.

Use the no parameter with this command to set the restricted-role value of the port to FALSE.

2.55.1 Command Syntax

```
(no) spanning-tree restricted-role
```

2.55.2 Command Mode

Interface mode

2.55.3 Default

The default restricted-role value is FALSE.

2.55.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree restricted-role
```

2.56 spanning-tree restricted-tcn

Use this command to set the restricted TCN value of the port to TRUE.

Use the no parameter with this command to set the restricted TCN value of the port to FALSE.

2.56.1 Command Syntax

```
(no) spanning-tree restricted-tcn
```

2.56.2 Command Mode

Interface mode

2.56.3 Default

The default restricted TCN value is FALSE.

2.56.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# spanning-tree restricted-tcn
```

2.57 traffic-class-table

Use this command to set the traffic class tables values, specifically, the user priority and number of supported traffic classes.

2.57.1 Command Syntax

`traffic-class-table user-priority USER num-traffic-classes NUMBER value VALUE <0-7>`

`USER = <0-7>` The user priority.

`NUMBER = <1-8>` The ID of traffic classes.

`VALUE = <0-7>`

2.57.2 Command Mode

Interface mode

2.57.3 Default

The default value for each user and traffic class is 0.

2.57.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# traffic-class-table user-priority 3 num-traffic-classes 4
value 5
```

2.58 user-priority

Use this command to set the default user priority associated with the Layer 2 interface.

2.58.1 Command Syntax

`(no) user-priority PRIORITY`

`PRIORITY <0-7>` Set the name of the bridge to use with this VLAN.

2.58.2 Command Mode

Interface mode

2.58.3 Examples

```
# configure terminal
(config)# interface eth1
(config-if)# user-priority 3
```

LACP Commands

3.1 Introduction

This chapter provides an alphabetized reference for each of the LACP commands.

3.2 channel-group mode

Use this command to add a port to a channel group specified by the channel group number (<1-65535>). This command enables link aggregation on a port, so that it may be selected for aggregation by the local system.

3.2.1 Command Syntax

`channel-group <1-65535> mode (active|passive)`

`<1-65535>` Specify a channel group number.

`active` Enable initiation of LACP negotiation on a port

`passive` Disable initiation of LACP negotiation on a port

3.2.2 Command Mode

Interface mode

3.2.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# channel-group 4 mode active
```

3.2.4 Related Commands

`no channel-group`

3.3 clear lacp counters

Use this command to clear all counters of all present LACP aggregators or a given LACP aggregator.

3.3.1 Command Syntax

`clear lacp (<1-65535>) counters`

`<1-65535>` Channel-group number.

3.3.2 Command Mode

Privileged Exec mode

3.3.3 Example

```
# clear lacp 2 counters
```

3.4 debug lacp

Use this command to turn on and turn off LACP debugging at various levels.

Use the no parameter with this command to turn off debugging.

3.4.1 Command Syntax

`debug lacp (all|event|packet)`

`all` all LACP debugging.

`event` set of debug options for LACP events.

`packet` LACP packets.

3.4.2 Command Mode

Configure mode

3.4.3 Examples

```
# debug lacp nsm
```

3.5 interface

Use this command to enter the Interface mode, and configure interface properties.

3.5.1 Command Syntax

`interface IFNAME`

`IFNAME` Name of the interface for which the properties are to be configured.

3.5.2 Command Mode

Configure mode

3.5.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)#
```

3.6 lacp port-priority

Set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the no parameter with this command to reset the priority of port to the default value (32768).

3.6.1 Command Syntax

`lacp port-priority <1-65535>`

`no lacp port-priority`

`<1-65535>` Specify the LACP port priority.

3.6.2 Command Mode

Interface mode

3.6.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# lacp port-priority 34
```

3.7 lacp system-priority

Use this command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups.

NOTE: Lower numerical values have higher priorities.

Use the no parameter with this command to reset the system priority of the local system to the default value (32768).

3.7.1 Command Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

<1-65535> LACP system priority. The default system priority is 32768.

3.7.2 Command Mode

Configure mode

3.7.3 Examples

```
# configure terminal
(config)# lacp system-priority 6700
```

3.8 lacp timeout

Set the short or long timeout on a port.

3.8.1 Command Syntax

`lacp timeout short|long`

`timeout` Number of seconds before invalidating a received LACP data unit (DU).

`short` LACP short timeout. Short timeout value is 3 seconds.

`long` LACP long timeout. Long timeout value is 90 seconds.

3.8.2 Command Mode

Interface mode

3.8.3 Default

The default is long timeout.

3.8.4 Usage

If the LACP_timeout bit (encoded in Actor_State and Partner_State fields) is set to 1, the short timeout takes effect; if set to 0, the long timeout takes effect.

3.8.5 Examples

The following sets the LACP short timeout on a port.

```
# configure terminal
(config)# interface eth0
(config-if)# lacp timeout short
```

3.9 load-balance field-select

This is an optional command which is executed on the ingress port. This command works in conjunction with the enhanced mode load-balancing configuration. It ensures better traffic distribution in topologies where the traffic is passing through two aggregator interfaces; one after the other.

NOTE: Load balancing offers better results, when the traffic has multiple flows.

3.9.1 Command Syntax

`load-balance field-select [extended|normal]`

`extended` Select extended hash field for load balancing in the enhanced mode.

`normal` Select normal hash field for load balancing in the enhanced mode.

3.9.2 Command Mode

Interface mode

3.9.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# load-balance field-select normal
```

3.10 load-balance extended-hash-seed

Use this command to configure extended hash-seed that has to be used in hashing algorithm.

3.10.1 Command Syntax

`load-balance extended-hash-seed <0-2147483647>`

3.10.2 Command Mode

Interface Mode

3.10.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# load-balance extended-hash-seed 100
```

3.10.4 Related Commands

`load-balance field-select`

3.11 no channel-group

Use this command to turn off link aggregation on a port.

3.11.1 Command Syntax

no channel-group

3.11.2 Command Mode

Interface mode

3.11.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# no channel-group
```

3.11.4 Related Commands

`channel-group mode`

3.12 port-channel load-balance

Use this command to configure LACP port-channel load-balancing and set port selection criteria (PSC) on an interface.

Use the no option with this command to remove the load-balancing configuration and unset PSC.

3.12.1 Command Syntax

`port-channel load-balance [dst-mac(enhanced MAC-OPTIONS)|src-mac(enhanced MAC-OPTIONS)|src-dstmac(enhanced MAC-OPTIONS)|dst-ip(enhanced IP-OPTIONS)|src-ip(enhanced IP-OPTIONS)|src-dst-ip(enhanced IP-OPTIONS)]`

`no port-channel load-balance`

`dst-mac` = destination MAC address-based load balancing

`src-mac` = source MAC address-based load balancing

`src-dst-mac` = source and destination MAC address-based load balancing

`dst-ip` = destination IP address-based load balancing

`src-ip` = source IP address-based load balancing

`src-dst-ip` = source and destination IP address-based load balancing

enhanced = enhanced load balancing

`MAC-OPTIONS` = vlanid, ethertype

`vlan-id` = apart from the specified MAC based load balancing, vlanid is also considered.

`ether-type` = apart from the specified MAC based load balancing, ethertype is also considered.

`IP-OPTIONS` = vlanid, protocolid, src-udp-tcp-port, dst-udp-tcp-port

`vlan-id` = apart from the specified IP based load balancing, vlanid is also considered.

`protocol-id` = apart from the specified IP based load balancing, protocol-id in IP header is also considered.

`src-udp-tcp-port` = apart from the specified IP based load balancing, source port in UDP/TCP header is also considered.

`dst-udp-tcp-port` = apart from the specified IP based load balancing, destination port in UDP/TCP header is also considered.

`ipv6-next-header` = apart from the specified IP based load balancing, IPv6 next header is also considered.

3.12.2 Usage

The load-balancing values map to macros on the underlying chipset, designated for specifying the port selection criteria (PSC).

You can use enhanced option to enable the usage of enhanced hash algorithm, which ensures better traffic distribution on the links. You can also specify `MAC-OPTIONS` (In case of MAC-based load balancing) or `IP-OPTIONS` (in case of IP-based load balancing), which is also considered while load balancing. The command fails, if the chipset does not support the enhanced option.

3.12.3 Command Mode

Interface mode

3.12.4 Examples

Example 1:

```
# configure terminal
(config)# interface eth1
(config-if)# port-channel load-balance src-dst-mac
```

Example 2:

```
# configure terminal
(config)# interface eth1
(config-if)# port-channel load-balance src-dst-mac enhanced
```

Example 3:

```
# configure terminal
(config)# interface eth1
(config-if)# port-channel load-balance src-dst-mac enhanced vlan-id
ether-type
```

3.13 show debugging lacp

Use this command to display the status of the debugging of the LACP system.

3.13.1 Command Syntax

```
show debugging lacp
```

3.13.2 Command Mode

Exec mode

3.13.3 Examples

```
# show debugging lacp
```

3.14 show etherchannel

Use this command to display etherchannels in a channel group.

3.14.1 Command Syntax

`show etherchannel <1-12>`

`<1-12>` Number that identifies the channel group

3.14.2 Command Mode

Exec mode

3.14.3 Example

show etherchannel 4

3.15 show etherchannel detail

Use this command to display detailed information about all LACP channels.

3.15.1 Command Syntax

`show etherchannel detail`

3.15.2 Command Mode

Privileged Exec mode

3.15.3 Examples

`# show etherchannel detail`

3.16 show etherchannel load-balance

Use this command to display load-balancing information of the etherchannels.

3.16.1 Command Syntax

`show etherchannel load-balance`

3.16.2 Command Mode

Privileged Exec mode

3.16.3 Example

A sample of the output of the command follows the command example.

```
# show etherchannel load-balance
% Lacp Aggregator: po1
Source and Destination IP address based load balancing
```

3.17 show etherchannel summary

Use this command to display a summary of all LACP channels.

3.17.1 Command Syntax

```
show etherchannel summary
```

3.17.2 Command Mode

Privileged Exec mode

3.17.3 Examples

```
# show etherchannel summary
```

3.18 show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

3.18.1 Command Syntax

```
show lacp-counter <1-65535>
```

<1-65535> Channel-group number.

3.18.2 Command Mode

Privileged Exec mode

3.19 show lacp sys-id

Use this command to display the LACP system ID and priority.

3.19.1 Command Syntax

`show lacp sys-id`

3.19.2 Command Mode

Privileged Exec mode

3.20 show port etherchannel

Use this command to show details of the LACP channel-group member port specified by the interface name (IFNAME).

3.20.1 Command Syntax

`show port etherchannel IFNAME`

`IFNAME` Name of the channel-group member interface

3.20.2 Command Mode

Privileged Exec mode

3.20.3 Examples

```
(config)# interface ge1
(config-if)# channel-group 1 mode active
# show port etherchannel ge1
```

3.21 show static-channel-group

Use this command to display all configured static aggregators and their corresponding member ports.

3.21.1 Command Syntax

`show static-channel-group`

3.21.2 Command Mode

Privileged Exec mode

3.21.3 Examples

```
# show static-channel-group
% Static Aggregator: sa1
% Member:
   eth0
   eth1
% Static Aggregator: sa2
% Member:
   eth2
```

3.22 static-channel-group

Use this command to create a static aggregator, or add a member port to an already-existing static aggregator. Use the `no` parameter with this command to detach the port from the static aggregator.

3.22.1 Command Syntax

`static-channel-group <1-12>`

`no static-channel-group`

`<1-12>` Channel group number.

3.22.2 Command Mode

Interface mode

3.22.3 Usage

This command adds the interface to the static aggregator with the specified key. If the aggregator does not exist, it is created, and the interface is added to it. The no prefix detaches the port from the static aggregator. If the port is the last member to be detached, the static aggregator is deleted.

3.22.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# static-channel-group 2
```

Bridge Commands

4.1 Introduction

This chapter contains the bridge commands.

4.2 bridge acquire

Use this command to enable a bridge to learn station location information for an instance. This helps in making forwarding decisions.

To disable learning, use the no parameter with this command.

4.2.1 Command Syntax

`bridge <1-32> acquire`

`no bridge <1-32> acquire`

<1-32> Bridge-group ID used for bridging.

4.2.2 Command Mode

Configure mode

4.2.3 Default

Learning is enabled by default for all instances.

4.2.4 Examples

```
# configure terminal
(config)# bridge 3 acquire
```

4.3 bridge address

Use this command to statically configure a bridge entry to forward or discard matching frames.

4.3.1 Command Syntax

`bridge <1-32> address MAC forward|discard IFNAME`

`no bridge <1-32> address MAC forward|discard IFNAME`

`<1-32>` Bridge-group ID used for bridging.

`MAC` A Media Access Control (MAC) address in the HHHH.HHHH.HHHH format.

`forward` Configure the bridge to forward matching frames

`discard` Configure the bridge to discard matching frames

`IFNAME` the interface on which the frame comes in.

4.3.2 Command Mode

Configure mode

4.3.3 Examples

```
# configure terminal
(config)# bridge 2 address 2222.2222.2222 forward eth0
```

4.4 bridge-group

Use this command to bind an interface with a bridge specified by the parameter.

By default, spanning tree is enabled on the interface. You can disable spanning-tree using the `spanning-tree disable` option.

4.4.1 Command Syntax

`(no) bridge-group <1-32> (spanning-tree disable)`

`<1-32>` Bridge-group ID used for bridging.

`spanning-tree disable` Disables spanning tree on the interface.

4.4.2 Command Mode

Interface mode

4.4.3 Examples

```
# configure terminal
(config)# interface eth1
(config-if)# bridge-group 2
```

4.5 bridge protocol ieee

Use this command to add a IEEE 802.1d Spanning Tree Protocol bridge. Use the no parameter to remove a bridge.

4.5.1 Command Syntax

`bridge <1-32> protocol ieee`

`no bridge <1-32>`

`<1-32>` Bridge-group ID used for bridging.

4.5.2 Command Mode

Configure mode

4.5.3 Default

There is no default value.

4.5.4 Usage

After creating a bridge instance, add interfaces to the bridge using the bridge-group command. Bring the bridge instance into operation with the no shutdown command in interface mode.

4.5.5 Examples

```
# configure terminal
(config)# bridge 3 protocol ieee
```

4.6 Bridge-group spanning-tree state

Use this command to configure a port in spanning tree block state. Use no command to disable this feature.

4.6.1 Command Syntax

`bridge-group <1-32> spanning-tree state (block|forward)`

`no bridge-group <1-32> spanning-tree state`

`<1-32>` Bridge-group ID used for bridging

`state` STP state of the interface

`block` Interface in block state

`forward` Interface in forward state

4.6.2 Command Mode

Interface mode

4.6.3 Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface ge1
(config-if)#bridge-group 1 spanning-tree state block
(config-if)#
```

4.7 bridge protocol ieee vlan-bridge

Use this command to add a VLAN bridge (according to the IEEE 802.1q Spanning Tree Protocol) to the spanning tree.

4.7.1 Command Syntax

`bridge <1-32> protocol ieee vlan-bridge`

<1-32> Bridge-group ID used for bridging.

4.7.2 Command Mode

Configure mode

4.7.3 Examples

`# configure terminal`

`(config)#` **`bridge 4 protocol ieee vlan-bridge`**

4.8 bridge protocol mstp

Use this command to create a multiple spanning-tree protocol (MSTP) bridge of a specified parameter.

Use the no parameter with this command to unmap the VLANs from a particular instance, and associate it back to the default instance of 0.

4.8.1 Command Syntax

`bridge <1-32> protocol mstp`

`no bridge <1-32>`

<1-32> Specify the bridge group ID.

4.8.2 Command Mode

Configure mode

4.8.3 Usage

The MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of “similar” MSTP bridges. The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration capability, while providing load balancing ability.

Using this command creates an instance of the spanning tree, and associates the VLANs specified with that instance.

A bridge created with this command forms its own separate region unless it is added explicitly to a region using the region name command.

4.8.4 Examples

```
# configure terminal
(config)# bridge 2 protocol mstp
```

4.9 bridge protocol rstp

Use this command to add an IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) bridge.

4.9.1 Command Syntax

`bridge <1-32> protocol rstp (ring)`

`<1-32>` Bridge-group ID used for bridging.

`ring` Optional. Add an RSTP bridge for a ring topology.

4.9.2 Command Mode

Configure mode

4.9.3 Usage

After creating a bridge instance, add interfaces to the bridge using the bridge-group command. Bring the bridge instance into operation with the no shutdown command in Interface mode.

4.9.4 Examples

```
# configure terminal
(config)# bridge 2 protocol rstp
```

4.10 bridge protocol rstp vlan-bridge

Use this command to add a VLAN bridge to the rapid spanning tree.

4.10.1 Command Syntax

bridge <1-32> protocol rstp vlan-bridge

<1-32> Bridge-group ID used for bridging.

4.10.2 Command Mode

Configure mode

4.10.3 Examples

```
# configure terminal
(config)# bridge 3 protocol rstp vlan-bridge
```

4.11 clear mac address-table bridge

Use this command to clear all of the:

- filtering database
- filtering database entries configured through CLI (static)
- multicast filtering database entries
- multicast filtering database entries for a given VLAN or interface
- static or multicast database entries based on a mac address

4.11.1 Command Syntax

`clear mac address-table (static|multicast) (address|vlan|interface) WORD bridge NAME`

`static` Filtering database entries configured through CLI.

`multicast` Multicast filtering database entries.

`address` Filtering database entries with the given MAC address.

`vlan` Filtering database entries for the given VLAN.

`interface` Filtering database entries for the given interface.

`WORD` Optional. One of the following:

MAC address when filtering database entries are cleared based on an MAC address

Interface name when filtering database entries are cleared based on an interface name

VLAN ID when filtering database entries are cleared based on VLANs. Value range is 1-4022

`NAME` Bridge name in the range <1-32>

4.11.2 Command Mode

Privileged Exec mode

4.11.3 Examples

This example shows how to clear all filtering database entries configured through CLI:

```
# clear mac address-table static bridge 1
```

This example shows how to clear multicast filtering database entries:

```
# clear mac address-table multicast bridge 1
```

This example shows how to clear all filtering database entries for a given interface:

```
# clear mac address-table static interface eth0 bridge 1
```

This example shows how to clear multicast filtering database entries for a given VLAN.

```
# clear mac address-table multicast vlan 2 bridge 1
```

This example shows how to clear static filtering database entries for a given MAC address:

```
# clear mac address-table static address 0202.0202.0202 bridge 1
```

4.12 clear mac address-table dynamic bridge

Use this command to clear the filtering database of all entries learned through bridge operation, or clear filtering database entries learned through bridge operation for a given MAC address, interface, or VLAN.

4.12.1 Command Syntax

`clear mac address-table dynamic bridge NAME`

`NAME` Bridge name <1-32>.

`clear mac address-table dynamic address|interface|vlan WORD bridge NAME`

`address` Filtering database entries for the given MAC address.

`interface` Filtering database entries for the given interface.

`vlan` Filtering database entries for the given VLAN.

`WORD` Optional. One of the following:

`MAC` address when filtering database entries are cleared based on an MAC address

Interface name when filtering database entries are cleared based on an interface name

VLAN ID when filtering database entries are cleared based on VLANs. Value range is 1-4022

4.12.2 Command Mode

Privileged Exec mode

4.12.3 Examples

This example shows how to clear all filtering database entries learned through bridge operation for a given MAC address.

```
# clear mac address-table dynamic address 0202.0202.0202 bridge 1
```

4.13 show bridge

Use this command to display the filtering database values.

4.13.1 Command Syntax

`show bridge`

4.13.2 Command Mode

Privileged Exec mode

4.13.3 Usage

The following is a sample output of the show bridge command.

```
# show bridge
bridge CVLAN SVLAN BVLAN port mac    fwd timeout
2        1                 eth2   0002.b328.5255 1 0
1        1                 eth1   0002.b328.5254 1 0
```

4.14 show interface switchport bridge

Use this command to display the characteristics of the Layer 2 interface with the current VLAN.

4.14.1 Command Syntax

```
show interface switchport bridge <1-32>
```

<1-32> Specify the ID of the bridge-group for which information is to be displayed.

4.14.2 Command Mode

Privileged Exec mode

4.14.3 Usage

The following is an output of this command displaying the characteristics of this interface on bridge 2.

```
# show interface switchport bridge 2
 Interface name          : eth5
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 2
 Configured vlans        :    2
 Interface name          : eth4
 Switchport mode         : access
 Ingress filter          : disable
```

```
Acceptable frame types : all
Vid swap               : disable
Default vlan           : 1
Configured vlans       :    1
```

4.14.4 Examples

```
# show interface switchport bridge 4
```

4.15 switchport

Use this command to set the switching characteristics of the Layer 2 protocols when using the SRstackware Hybrid Layer 2/Layer 3 solution.

Use the no parameter with this command to revert to the default behavior.

4.15.1 Command Syntax

```
(no) switchport
```

4.15.2 Command Mode

Interface mode

4.15.3 Usage

In case of SRstackware Hybrid L2/ L3, it is important to understand that, by default, all interfaces are configured as routed interfaces. and if you want to change the behavior of a port from a switched port to a routed port, you must explicitly configure this using the no switchport command in the interface mode.

4.15.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# no switchport
```

GMRP Commands

5.1 Introduction

This chapter contains the commands to configure specific VLANs or all VLANs on Layer 2 bridges or switches using the GARP Multicast Registration Protocol. GMRP supports a mechanism to enable bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment, and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services. The operation of GMRP relies upon the services provided by the GARP (Generic Attribute Registration Protocol).

5.2 clear gmrp statistics

Use this command to clear GMRP statistics for a given VLAN or all the VLANs configured on the Layer 2 switch.

5.2.1 Command Syntax

`clear gmrp statistics [all|vlan VLAN-ID] bridge <1-32>`

`all` Clear GMRP statistics for all the VLANs.

`VLAN-ID = vlanid <1 to 4022>` Clear GMRP statistics for the particular VLAN_ID.

5.2.2 Command Mode

Privileged Exec mode

5.2.3 Default

This default clearing is for all the configured VLANs

5.2.4 Examples

This example shows how to clear the GMRP statistics for a given VLAN 12.

```
# clear gmrp statistics vlan 12 bridge 2
```

This example shows to clear the GMRP statistics for all the configured VLANs on a bridge.

```
# clear gmrp statistics all bridge 2
```

5.3 debug gmrp

Use this command to display various types of data on the console. Use the all parameter to display all types of debugging information on the console, or use any combination of the other parameters to display desired data on the console. Use the no parameter to turn off a specific type of debugging.

5.3.1 Command Syntax

```
(no) debug gmrp event|cli|timer|packet|all
event use this parameter to echo events to the console.
cli use this parameter to echo commands to the console.
timer use this parameter to echo the time start to the console.
packet use this parameter to echo packet contents to the console.
all to echo all of the above data types to the console.
```

5.3.2 Command Mode

Configure mode

5.3.3 Default

If this command is not used, no debugging data is displayed on the console.

5.3.4 Examples

This example shows set debugging for commands and packets:

```
# configure terminal
(config)# debug gmrp cli
```

5.4 set gmrp bridge

Use this command to enable/disable GMRP globally on a particular bridge. This command does not enable/disable GMRP in all ports of the bridge. After enabling GMRP globally, use the set port gmrp command to enable GMRP on individual ports of the bridge.

NOTE: Bridge should be vlan-aware to enable GMRP.

5.4.1 Command Syntax

`set gmrp enable|disable bridge <1-32>`

`enable` Enable GMRP on Layer 2 switch.

`disable` Disable GMRP on Layer 2 switch

`<1-32>` Bridge-group ID used for bridging.

5.4.2 Command Mode

Configure mode

5.4.3 Default

If this command is not used, GMRP is disabled.

5.4.4 Usage

It is important to know that GMRP cannot be enabled if IGMP Snooping is enabled, or if GMRP has already been configured for a particular VLAN.

5.4.5 Examples

To enable GMRP on a Layer 2 switch for bridge 2:

```
# configure terminal
(config)# set gmrp enable bridge 2
GMRP is enabled for bridge 2
```

To enable GMRP on a Layer 2 switch on bridge 3 when IGMP Snooping is enabled:

```
# configure terminal
(config)# set gmrp enable bridge 3
```

NOTE: First disable IGMP Snooping, then enable GMRP on bridge 3.

5.4.6 Related Commands

`set gmrp, set port gmrp`

5.5 set gmrp extended-filtering bridge

Use this command to enable or disable extended filtering on a bridge as per Table 8-7 of IEEE802.1Q-2003.

5.5.1 Command Syntax

`set gmrp extended-filtering enable|disable bridge BRIDGE NAME <1-32>`

`enable` Enables extended filtering services on the bridge

`disable` Disabled extended filtering services on the bridge

BRIDGE NAME Identifies a specific bridge

`<1-32>` Bridge-group ID used for bridging

5.5.2 Command Mode

Configure mode

5.5.3 Default

Extended filtering is disabled on a GMRP-enabled bridge.

5.5.4 Examples

Enable extended filtering services on bridge 1:

```
# set gmrp extended-filtering enable bridge 1
```

Disable extended filtering services on bridge 1:

```
# set gmrp extended-filtering disable bridge 1
```

5.6 set gmrp fwdall

Use this command to set the GMRP forward all option for an interface.

5.6.1 Command Syntax

`set gmrp fwdall enable|disable IF_NAME`

`enable` Enable the forward all option for this interface

`disable` Disable the forward all option for this interface

`IF_NAME` The identity of the interface

5.6.2 Command Mode

Configure mode

5.6.3 Default

If this command is not used, the default setting is GMRP disabled.

5.6.4 Examples

To enable GMRP forwarding on a Layer 2 switch for a particular interface:

```
IPInfusion (enable)> set gmrp fwdall enable eth1
```

5.7 set gmrp registration

Use this command to set GMRP registration type for all ports for a given bridge.

5.7.1 Command Syntax

`set gmrp registration normal|fixed|forbidden PORT-NAME`

`normal` Set dynamic GMRP multicast registration and deregistration on the port.

`fixed` Determine that the multicast groups currently registered on the switch are applied to the port, but that subsequent registrations or deregistrations do not affect the port. This means that none of the registered multicast groups on the port are to be de-registered based on GARP timers.

`forbidden` Indicates that all GMRP multicasts are deregistered, and prevents further GMRP multicast registration on the port.

`PORT-NAME` Defines a text string used as the name of the interface in ASCII format. Valid number of characters is between 1 and 16.

5.7.2 Command Mode

Configure mode

5.7.3 Default

The default is normal registration for all the ports

5.7.4 Usage

To deregister a multicast port, the port must be in the normal registration mode.

5.7.5 Examples

This example shows how to set the port to normal registration:

```
# set gmrp registration normal eth0
```

GMRP Registration is set to normal for eth0.

5.8 set gmrp timer

Use this command to set the values for the GMRP Join, Leave, and Leaveall timers for a specified bridge.

5.8.1 Command Syntax

`set gmrp timer [join |leave |leaveall] TIMER_VALUE IFNAME`

`join` Join timer

`leave` Leave timer

`leaveall` Leaveall timer

`TIMER_VALUE` Timer value in hundredths of a second.

`IFNAME` Specify the name of the interface.

5.8.2 Command Mode

Configure mode

5.8.3 Default

The default for the join timer is 200 milliseconds (ms), for the leave timer it is 600 milliseconds, and for the leaveall timer it is 10000 ms.

5.8.4 Usage

The relationship for the timer values are as follows:

Leave timer must be greater than, or equal to, three times the join timer.

Leaveall timer must be greater than the leave timer.

5.8.5 Examples

This example shows how to set the join timers for all ports and all VLANs.

```
# configure terminal
(config)# set gmrp timer join 100 eth0
GARP Join timer value is set to 100 centiseconds
```

5.9 set gmrp vlan

Use this command to enable or disable GMRP on a Layer 2 switch for a particular VLAN.

5.9.1 Command Syntax

`set gmrp enable|disable bridge <1-32> vlan <1-4022>`

`enable` Enable GMRP on Layer 2 switch for the specified VLAN.

`disable` Disable GMRP on Layer 2 switch for the specified VLAN.

`<1-32>` Bridge-group ID used for bridging.

`<1-4022>` VLAN number on which GMRP is to be enabled.

5.9.2 Command Mode

Configure mode

5.9.3 Usage

GMRP on a VLAN cannot be enabled if IGMP Snooping is enabled, or if GMRP is globally enabled on a bridge.

5.9.4 Examples

To enable GMRP on a Layer 2 switch for a bridge 2 and VLAN 2:

```
# configure terminal
(config)# set gmrp enable bridge 2 vlan 2
```

To disable GMRP on a Layer 2 switch for a bridge 2 and VLAN 2:

```
# configure terminal
(config)# set gmrp disable bridge 2 vlan 2
```

5.10 set port gmrp

Use this command to enable or disable GMRP on a particular port in all VLANs or all ports in a bridge.

5.10.1 Command Syntax

`set port gmrp enable|disable all|IFNAME`

`enable` Enable GMRP on Layer 2 switch port

`disable` Disable GMRP on Layer 2 switch port

`all` All ports added to recently configured bridge

`IFNAME` Specify the name of the interface.

5.10.2 Command Mode

Configure mode

5.10.3 Default

By default, GMRP is disabled.

5.10.4 Usage

GMRP on a port cannot be enabled for all VLANs if GMRP has already been configured for a particular VLAN for the port.

5.10.5 Examples

This example shows how to enable GMRP on a particular port in all VLANs on a specified bridge.

```
# configure terminal
(config)# set port gmrp enable eth0
```

GMRP enabled on port eth0

```
# configure terminal
(config)# set port gmrp enable all
GMRP enabled on all ports added to recently configured bridge
```

5.11 set port gmrp vlan

Use this command to enable or disable GMRP on a particular port in a particular VLAN.

5.11.1 Command Syntax

`set port gmrp enable|disable IFNAME vlan <1-4022>`

`enable` Enable GMRP on Layer 2 switch port

`disable` Disable GMRP on Layer 2 switch port

`IFNAME` Specify the name of the interface.

`<1-4022>` VLAN number on which GMRP is to be enabled.

5.11.2 Command Mode

Configure mode

5.11.3 Usage

GMRP cannot be enabled on a VLAN basis if it has been enabled for all VLANs for the port.

GMRP cannot be enabled for a port for a VLAN if GMRP is not enabled for the VLAN for the bridge.

5.11.4 Examples

This example shows how to enable GMRP on a specified port (eth0) in VLAN 2.

```
# configure terminal
(config)# set port gmrp enable eth0 vlan 2
GMRP enabled on port eth0 and vlan 2
```

5.12 show debugging gmrp

Use this command to display the status of the debugging of the GMRP system.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see *Chapter 1, Command Line Interface Environment*.

5.12.1 Command Syntax

```
show debugging gmrp
```

5.12.2 Command Mode

Exec and Privileged Exec mode

5.12.3 Examples

```
# show debugging gmrp
```

5.13 show gmrp configuration bridge

To display GMRP related configuration information for a given bridge.

To modify the lines displayed, use the | (output modifier token) and to save the output to a file, use the > (output redirection token). For more information, see *Chapter 1, Command Line Interface Environment*.

5.13.1 Command Syntax

```
show gmrp configuration bridge <1-32>
```

<1-32> Bridge-group ID used for bridging.

5.13.2 Command Mode

Privileged Exec mode

5.13.3 Default

None

5.13.4 Usage

The following is an output of this command displaying GMRP related configuration information:

```
# show gmrp configuration bridge 2
Global GMRP Configuration for bridge :2
GMRP Feature: Enabled
GMRP Timers (centiseconds):
Join:          20
Leave:         60
Leave All:     1000
Port based GMRP Configuration:
GMRP Status    Registration    Forward All    Port
-------------------------------------------------
Enabled        Normal          Disabled        eth4
Enabled        Normal          Disabled        eth5
```

where:

- `GMRP Status` Status of GMRP for the particular port.
- `Registration` Registration status of GMRP for the particular port.
- `Forward All` Forward All status of GMRP for the particular port.
- `Ports` Ports that have GMRP Enabled or Disabled.

5.13.5 Examples

```
show gmrp configuration bridge 3
```

5.14 show gmrp machine bridge

Use this command to display the state machine for GMRP, for a particular bridge.

5.14.1 Command Syntax

```
show gmrp machine bridge <1-32>
```

<1-32> Bridge-group ID used for bridging.

5.14.2 Command Mode

Exec and Privileged Exec modes

5.14.3 Usage

The following is an output of this command displaying the GMRP state machine.

```
# show gmrp machine bridge 2
port = eth0    VLAN = 1     applicant state[0] = VO  registrar state[0] = MT
                            applicant state[1] = VO  registrar state[1] = MT
port = eth1    VLAN = 1     applicant state[0] = VO  registrar state[0] = MT
                            applicant state[1] = VO  registrar state[1] = MT
```

5.14.4 Examples

```
# show gmrp machine bridge 2
```

5.15 show gmrp statistics

To display the GMRP related statistics.

5.15.1 Command Syntax

```
show gmrp statistics
```

5.15.2 Command Mode

Privileged Exec mode

5.15.3 Examples

The following is an output of this command displaying GMRP statistics.

```
# show gmrp statistics
GMRP Statistics for bridge b vlan 1
-------------------------------------------------
Total GMRP packets Received:      0
Join Empties:                     0
Join Ins:                         0
Leave Empties:                    0
Leave Ins:                        0
Empties:                          0
Total GMRP packets Transmitted:   0
Join Empties:                     0
Join Ins:                         0
Leave Empties:                    0
Leave Ins:                        0
Empties:                          0
```

5.16 show gmrp timer

To display GMRP timer values on a specified interface.

5.16.1 Command Syntax

`show gmrp timer IFNAME`

`IFNAME` Specify the name of the interface.

5.16.2 Command Mode

Privileged Exec mode

5.16.3 Usage

The following is an output of this command displaying the GMRP timer values for interface eth4.

```
# show gmrp timer eth4
Timer           Timer Value (centiseconds)
----------------------------------------
Join                20
Leave               60
Leave All           1000
```

5.16.4 Examples

```
# show gmrp timer eth0
```

GVRP Commands

6.1 Introduction

This chapter contains the SRstackware® GARP VLAN Registration Protocol commands. GVRP provides a method to dynamically share VLAN information and configure the needed VLANs. For example, to add a switch port to a VLAN, only the end port need be reconfigured, and all necessary VLAN trunks are dynamically created on the other GVRP-enabled switches. GVRP employs the GARP Information Declaration (GID) and GARP Information Propagation (GIP) that supply the common state machine descriptions and the common information propagation mechanisms defined for use in GARP-based applications

6.2 clear gvrp statistics

Use this command to clear GVRP statistics for all VLANs or a specific VLAN.

6.2.1 Command Syntax

`clear gvrp statistics [all|bridge <1-32>]`

`clear gvrp statistics <IFNAME>`

`<1-32>` Bridge-group ID used for bridging.

`IFNAME` Interface name

6.2.2 Command Mode

Privileged Exec mode

6.2.3 Examples

```
# clear gvrp statistics all
# clear gvrp statistics bridge 1
# clear gvrp statistics ge1
```

6.3 debug gvrp

Use this command to debug GVRP events, packets, timer starts, and commands, sending output to the console.

Use the no parameter to turn off debugging.

6.3.1 Command Syntax

`(no) debug gvrp [all|event|cli|timer|packet]`

`all` Turns on or off debugging for all levels.

`event` Turns on or off debugging for GVRP events.

`cli` Turns on or off debugging for GVRP commands.

`timer` Turns on or off debugging for GVRP timer starts.

`packet` Turns on or off debugging for GVRP packets.

6.3.2 Command Mode

Configure mode

6.3.3 Examples

```
# configure terminal
(config)# debug gvrp all
```

6.4 set gvrp applicant

Use this command to set the GVRP applicant state to normal or active.

6.4.1 Command Syntax

`set gvrp applicant state [active|normal] IFNAME`

`active` Active state

`normal` Normal state

`IFNAME` Name of the interface

6.4.2 Command Mode

Configure mode

6.4.3 Examples

```
# configure terminal
(config)# set gvrp applicant state active eth0
```

6.5 set gvrp bridge

Use this command to enable (set) or disable (reset) GVRP globally for the bridge instance. This command does not enable or disable GVRP in all ports of the bridge. After enabling GVRP globally, use the set port gvrp command to enable GVRP on individual ports of the bridge.

6.5.1 Command Syntax

```
set gvrp enable bridge <1-32>
set gvrp disable bridge <1-32>
```

<1-32> Bridge-group ID used for bridging.

6.5.2 Command Mode

Configure mode

6.5.3 Examples

```
# configure terminal
(config)# set gvrp enable bridge 2
```

6.6 set gvrp dynamic-vlan-creation bridge

Use this command to enable and disable dynamic VLAN creation for a specific bridge instance.

6.6.1 Command Syntax

`set gvrp dynamic-vlan-creation enable bridge <1-32>`

`set gvrp dynamic-vlan-creation disable bridge <1-32>`

<1-32> Bridge-group ID used for bridging.

6.6.2 Command Mode

Configure mode

6.6.3 Examples

```
# configure terminal
(config)# set gvrp dynamic-vlan-creation enable bridge 2
(config)# set gvrp dynamic-vlan-creation disable bridge 2
```

6.7 set gvrp registration

Use this command to set GVRP Registration to normal, fixed, and forbidden Registration mode for a given port.

6.7.1 Command Syntax

`set gvrp registration [normal|fixed|forbidden] IF_NAME`

`normal` Specify dynamic GVRP multicast registration and deregistration on the port.

`fixed` Specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or de-registrations do not affect the port. Any registered multicast groups on the port are not de-registered based on the GARP timers.

`forbidden` Specify that all GVRP multicasts are de-registered, and prevent any further GVRP multicast registration on the port.

`IF_NAME` The name of the interface.

6.7.2 Command Mode

Configure mode

6.7.3 Examples

```
# configure terminal
(config)# set gvrp registration fixed eth0
```

6.8 set gvrp timer

Use this command to set GVRP timers for a specific interface.

6.8.1 Command Syntax

`set gvrp timer [join|leave|leaveall] TIMER_VALUE IF_NAME`

`join` To set the timer for joining the group

`leave` To set the timer for leaving a group

`leaveall` To set the time for leaving all groups

`TIMER_VALUE = <1-65535>` The timer value in hundredths of a second

`IF_NAME` The name of the interface.

6.8.2 Command Mode

Configure mode

6.8.3 Examples

```
# configure terminal
(config)# set gvrp timer leave 245 eth0
```

6.9 set port gvrp

Use this command to enable or disable GVRP on a port or all ports in a bridge.

6.9.1 Command Syntax

`set port gvrp {enable|disable] [all|IFNAME]`

`enable` Enable GVRP on all ports on a bridge or a specific interface

`disable` Disable GVRP on all ports on a bridge or a specific interface

`all` All ports added to recently configured bridge.

`IFNAME` The name of the interface.

6.9.2 Command Mode

Configure mode

6.9.3 Examples

```
# configure terminal
(config)# set port gvrp enable eth0
# configure terminal
(config)# set port gvrp enable all
```

6.10 show debugging gvrp

Use this command to display the status of the debugging for the GVRP system.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see *Chapter 1, Command Line Interface Environment*.

6.10.1 Command Syntax

`show debugging gvrp`

6.10.2 Command Mode

Exec and Privileged Exec mode

6.10.3 Examples

```
# show debugging gvrp
```

6.11 show gvrp configuration bridge

Use this command to display GVRP configuration bridge data for a specified bridge instance.

6.11.1 Command Syntax

```
show gvrp configuration (bridge <1-32>)
```

<1-32> Bridge-group ID used for bridging.

6.11.2 Command Mode

Exec and Privileged Exec mode

6.11.3 Usage

The following is an output of this command displaying the GVRP configuration for bridge 3.

```
# show gvrp configuration bridge 3
Global GVRP Configuration for bridge 3:
GVRP Feature: Enabled
Dynamic Vlan Creation: Disabled
Port based GVRP Configuration:
Timers(centiseconds)
Port    GVRP Status    Registration     Applicant   Join   Leave LeaveAll
------------------------------------------------------------------------
-
eth4    Enabled        Normal           Normal      20      60    1000
eth5    Enabled        Normal           Normal      200    600   10000
```

6.11.4 Examples

```
# show gvrp configuration bridge 2
```

6.12 show gvrp machine bridge

Use this command to display the state machine for GVRP.

6.12.1 Command Syntax

`show gvrp machine bridge <1-32>`

`<1-32>` Bridge-group ID used for bridging.

6.12.2 Command Mode

Exec and Privileged Exec modes

6.12.3 Usage

The following is an output of this command displaying the GVRP state machine.

```
# show gvrp machine bridge 2
  port = eth5  applicant state = QA   registrar state = INN
  port = eth4  applicant state = QA   registrar state = INN
```

6.12.4 Examples

```
# show gvrp machine bridge 2
```

6.13 show gvrp statistics

Use this command to display a statistical summary for a bridge.

6.13.1 Command Syntax

`show gvrp statistics IFNAME`

`IFNAME` Name of the port.

6.13.2 Command Mode

Exec and Privileged Exec mode

6.13.3 Usage

The following is an output of this command displaying a statistical summary for bridge 2.

```
# show gvrp statistics
Bridge: b
Port      JoinEmpty    JoinIn   LeaveEmpty     LeaveIn     Empty
------------------------------------------------------------------------
eth5      RX           0          2          0        0       0
          TX           0          0          0        0       0
eth4      RX           0          1          0        0       1
          TX           0          0          0        0       0
```

6.13.4 Examples

```
# show gvrp statistics eth0
```

6.14 show gvrp timer

Use this command to display data for the timers.

6.14.1 Command Syntax

```
show gvrp timer IF_NAME
```

6.14.2 Command Mode

Exec and Privileged Exec mode

6.14.3 Usage

The following show output displays data for timer on interface eth4.

```
# show gvrp timer eth4
Timer           Timer Value (centiseconds)
----------------------------------------
Join                20
Leave               60
Leave All           1000
```

VLAN Commands

7.1 Introduction

This chapter contains the CLI commands used to manage VLANs.

7.2 VLAN Commands

The following sections list the VLAN commands.

7.2.1 show vlan

Use this command to display information about a particular VLAN by specifying the VLAN ID. It displays information for all the bridges configured.

7.2.1.1 Command Syntax

`show vlan <2-4022>`

<2-4022> VLAN ID.

7.2.1.2 Command Mode

Privileged Exec mode

7.2.1.3 Examples

`# show vlan 2`

```
The following is an output of this command displaying information about
VLAN 2.
Bridge Group  VLAN ID   Name           State       Member ports
([u]-Untagged, [t]-Tagged)
------------ --------- --------------- ----------- ---------------------
 1            2        VLAN0002        active      [u]eth1 [t]eth2
```

7.2.2 show vlan all bridge

Use this command to display information about all VLAN connections on a bridge.

7.2.2.1 Command Syntax

`show vlan all bridge <1-32>`

<1-32> Bridge group ID

7.2.2.2 Command Mode

Privileged Exec mode

7.2.2.3 Examples

`# show vlan all bridge 1`

The following is a sample output of this command displaying all VLANs on bridge 1.

```
Bridge          VLAN ID  Name           State   Member ports
                                                (u)-Untagged, (t)-Tagged
=============== ======= ============== ======= ========================
1            1      default        ACTIVE  fe17(u) po1(t) fe43(t) fe44(t)
Bridge          VLAN ID  Name     State   Member ports
                                                (u)-Untagged, (t)-Tagged
=============== ======= ============== ======= ========================
1               11      VLAN0011        ACTIVE  po1(t)
```

7.2.3 show vlan brief

Use this command to display information about all VLANs configured for all bridges.

7.2.3.1 Command Syntax

`show vlan brief`

7.2.3.2 Command Mode

Privileged Exec mode

7.2.3.3 Examples

 # show vlan brief

The following is sample output from this command displaying the status of all VLANs on bridge 1:

```
Bridge          VLAN ID  Name   State Member ports
                                                (u)-Untagged, (t)-Tagged
=============== ======= ================ ====== ========================
1             1      default        ACTIVE  fe17(u) po1(t) fe43(t) fe44(t)
Bridge          VLAN ID  Name             State  Member ports
                                                (u)-Untagged, (t)-Tagged
=============== ======= ================ ====== ========================
1               11      VLAN0011         ACTIVE  po1(t)
```

7.2.4 show vlan classifier group

Use this command to display information about all configured VLAN classifier groups or a specific group.

7.2.4.1 Command Syntax

`show vlan classifier group (<1-16>)`

`<1-16>` VLAN classifier group identifier

7.2.4.2 Command Mode

Exec mode

7.2.4.3 Usage

If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

7.2.4.4 Examples

 # show vlan classifier group 1

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

7.2.5 show vlan classifier interface group

Use this command to display information about all interfaces configured for a VLAN group or all the groups.

7.2.5.1 Command Syntax

`show vlan classifier interface group (<1-16>)`

<1-16> VLAN classifier interface group identifier

7.2.5.2 Command Mode

Exec mode

7.2.5.3 Usage

If a group ID is not specified, all interfaces configured for all VLAN classifier groups are shown. If a group ID is specified, the interfaces configured for this VLAN classifier group are shown.

7.2.5.4 Examples

This example displays all interfaces for all VLAN classifier groups:

```
# show vlan classifier interface group
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
vlan classifier group 2 interface fe5
vlan classifier group 3 interface fe7
```

This example displays all interfaces for VLAN classifier group 1

```
# show vlan classifier interface group 1
vlan classifier group 1 interface fe2
vlan classifier group 1 interface fe3
```

7.2.6 show vlan classifier rule

Use this command to display information about all configured VLAN classifier rules or a specific rule.

7.2.6.1 Command Syntax

`show vlan classifier rule (<1-256>)`

<1-256> VLAN classifier rule identifier

7.2.6.2 Command Mode

Exec mode and Privileged Exec mode

7.2.6.3 Usage

If a rule ID is not specified, all configured VLAN classifier rules are shown. If a rule ID is specified, a specific configured VLAN classifier rule is shown.

7.2.6.4 Examples

```
# show vlan classifier rule 1
vlan classifier group 1 add rule 1
```

7.2.7 show vlan dynamic bridge

Use this command to display information about all dynamic VLANs on a bridge.

7.2.7.1 Command Syntax

`show vlan dynamic bridge <1-32>`

<1-32> **Bridge-group ID.**

7.2.7.2 Command Mode

Privileged Exec mode

7.2.7.3 Examples

The following is a sample output of this command displaying dynamic VLANs on bridge 1.

```
# show vlan dynamic bridge 1
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
=============== ======= ================ ======= ========================
1               11       *VLAN0011       ACTIVE  fe33(t)
1               14       *VLAN0014       ACTIVE  fe33(t)
```

7.2.8 show vlan static bridge

Use this command to display information about all static VLANs on a bridge.

7.2.8.1 Command Syntax

`show vlan static bridge <1-32>`

<1-32> Bridge-group ID.

7.2.8.2 Command Mode

Privileged Exec mode

7.2.8.3 Examples

The following is a sample output of this command displaying static VLANs on bridge 1.

```
# show vlan static bridge 1
Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
=============== ======= ================ ==============================
1            1      default         ACTIVE  fe17(u) po1(t) fe43(t)fe44(t)
Bridge          VLAN ID Name             State   Member ports
                                                 (u)-Untagged, (t)-Tagged
=============== ======= ================ ==============================
1               11      VLAN0011         ACTIVE po1(t)
```

7.2.9 switchport access vlan

Use this command to change the default VLAN on the current interface.

Use the no parameter to remove a previously created VLAN.

7.2.9.1 Command Syntax

`switchport access vlan VLANID`

`no switchport access vlan`

`VLANID = < 2-4022>` The default VLAN ID for the interface.

7.2.9.2 Command Mode

Interface mode

7.2.9.3 Usage

IP Infusion does not recommend the use of VLANID identifier 1 because of interoperability issues with other vendors' equipment.

7.2.9.4 Examples

This example shows the steps of a typical VLAN session, creating and destroying a VLAN.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport access vlan 3
...
(config)# interface eth0
(config-if)# no switchport access vlan
```

7.2.9.5 Related Commands

`show vlan`

7.2.10 switchport hybrid allowed vlan

Use this command to set the switching characteristics of the Layer 2 interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

Use the no parameter to turn off allowed hybrid switching.

7.2.10.1 Command Syntax

```
switchport hybrid allowed vlan all
switchport hybrid allowed vlan none
switchport hybrid allowed vlan add VLANID (egress-tagged
[enable|disable])
switchport hybrid allowed vlan remove VLANID
switchport hybrid allowed vlan except VLANID
no switchport hybrid vlan
```

`all` Allow all VLANs to transmit and receive through the Layer 2 interface.

none Allow no VLANs to transmit and receive through the Layer 2 interface.

add Add a VLAN to the member set.

`remove` Remove a VLAN from the member set.

except All VLANs except the VLAN for which the ID is specified, are part of its ports member set.

VLANID = <2-4022> The ID of the VLAN or VLANs that will be added to, or removed from, the Layer 2 interface.

For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.

For a VLAN list, specify the VLAN numbers separated by commas.

NOTE: Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

egress-tagged

enable Enable egress tagging for outgoing frames

disable Disable egress tagging for outgoing frames

7.2.10.2 Command Mode

Interface mode

7.2.10.3 Examples

The following shows adding a single VLAN to the member set.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2 egress-tagged enable
```

The following shows adding a range of VLANs to the member set.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2-4 egress-tagged enable
```

The following shows adding a list of VLANs to the member set.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport hybrid allowed vlan add eg
switchport hybrid allowed vlan add 2,3,4 egress-tagged enable
```

7.2.11 switchport hybrid vlan

Use this command to set the switching characteristics of the Layer 2 interface to hybrid.

Use the no parameter to turn off hybrid switching (no switchport hybrid), or add the Layer 2 interface to the default VLAN (no switchport hybrid vlan).

7.2.11.1 Command Syntax

`switchport hybrid vlan VLANID`

`VLANID` The ID of the VLAN that will be added to, or removed from, the Layer 2 interface

`no switchport hybrid`

Turns off the Layer 2 switching characteristic.

`no switchport hybrid vlan`

Adds the Layer 2 interface to the default VLAN.

7.2.11.2 Command Mode

Interface mode

7.2.11.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport hybrid vlan 18
```

7.2.12 switchport mode access

Use this command to set the switching characteristics of the Layer 2 interface to access mode, and classify untagged frames only. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Use the no parameter with this command to reset the mode of the Layer 2 interface to access (default).

7.2.12.1 Command Syntax

`switchport mode access (ingress-filter [enable|disable])`

`no switchport mode`

`ingress-filter` Set the ingress filtering for the received frames.

`enable` Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

`disable` Turn off ingress filtering to accept frames that do not meet the classification criteria.

7.2.12.2 Command Mode

Interface mode

7.2.12.3 Default

The result of not using this command is that ingress filtering is off, and that all frame types are classified and accepted.

Using this command without the ingress-filter parameter causes this command to use the default values.

7.2.12.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport mode access ingress-filter enable
```

7.2.13 switchport mode hybrid

Use this command to set the switching characteristics of the Layer 2 interface as hybrid, and classify both tagged and untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Use the no parameter to reset the mode of the Layer 2 interface to access (default).

7.2.13.1 Command Syntax

`switchport mode hybrid`

`switchport mode hybrid ingress-filter [enable|disable]`

`switchport mode hybrid acceptable-frame-type vlan-tagged`

`no switchport mode`

`ingress-filter` Set the ingress filtering for the frames received.

`enable` Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

`disable` Turn off ingress filtering to accept frames that do not meet the classification criteria.

`acceptable-frame-type` Set the Layer 2 interface acceptable frame types. This processing occurs after VLAN classification.

`vlan-tagged` Accept only classified frames which belong to the port's member set.

7.2.13.2 Command Mode

Interface mode

7.2.13.3 Default

The result of not using this command is that ingress filtering is off, and that all frame types are classified and accepted.

Using this command without either ingress-filter or acceptable-frame-type parameters causes this command to use the default values for each.

7.2.13.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport mode hybrid acceptable-frame-type vlan-tagged
```

7.2.14 switchport mode trunk

Use this command to set the switching characteristics of the Layer 2 interface as trunk, and specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Use the no parameter to reset the mode of the Layer 2 interface to access (default).

7.2.14.1 Command Syntax

`switchport mode trunk (ingress-filter [enable|disable])`

`no switchport mode`

`ingress-filter` Set the ingress filtering for the frames received.

`enable` Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

`disable` Turn off ingress filtering to accept frames that do not meet the classification criteria.

7.2.14.2 Command Mode

Interface mode

7.2.14.3 Default

The result of not using this command is that ingress filtering is off, and that all frame types are classified and accepted.

Using this command without the ingress-filter parameter causes this command to use the default values.

7.2.14.4 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport mode trunk ingress-filter enable
```

7.2.15 switchport trunk allowed vlan

Use this command to set the switching characteristics of the Layer 2 interface to trunk. The all parameter indicates that any VLAN ID is part of its port's member set. The none parameter indicates that no VLAN ID is configured on this port. The add and remove parameters will add and remove VLAN IDs to/from the port's member set.

Use the no parameter to remove all VLAN IDs configured on this port.

7.2.15.1 Command Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add VLANID
switchport trunk allowed vlan remove VLANID
switchport trunk allowed vlan except VLANID
no switchport trunk native vlan
```

`all` Allow all VLANs to transmit and receive through the Layer 2 interface.

none Allow no VLANs to transmit and receive through the Layer 2 interface.

add Add a VLAN to transmit and receive through the Layer 2 interface.

remove Remove a VLAN from transmit and receive through the Layer 2 interface.

except All VLANs, except the VLAN for which the ID is specified, are part of its ports member set.

VLANID <2-4022> The ID of the VLAN or VLANs that will be added to, or removed from, the Layer 2 interface. A single VLAN, VLAN range, or VLAN list can be set.

For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.

For a VLAN list, specify the VLAN numbers separated by commas.

NOTE: Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

7.2.15.2 Command Mode

Interface mode

7.2.15.3 Examples

The following example shows adding a single VLAN to the port's member set.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport trunk allowed vlan add 2-4
```

The following shows adding a list of VLANs to the port's member set.

```
# configure terminal
(config)# interface eth0
(config-if)# switchport trunk allowed vlan add 2,3,4
```

7.2.16 switchport trunk native vlan

Use this command to configure native VLANs for this port. The native VLAN is used for classifying the incoming untagged packets.

Use the no parameter to revert the native VLAN to the default VLAN ID 1.

7.2.16.1 Command Syntax

`switchport trunk native vlan VLANID`

`no switchport trunk native vlan`

`VLANID <1-4022>` The ID of the VLAN that will be used to classify the incoming untagged packets. The VLAN ID must be a part of the VLAN member set of the port.

7.2.16.2 Command Mode

Interface mode

7.2.16.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport trunk native vlan 2
```

7.2.17 switchport vlan-stacking customer-edge-port ethertype VALUE

Use this command to enable VLAN stacking and set the switching characteristics of the Layer 2 interface to customer-edge port.

Use the no parameter to disable VLAN stacking of the Layer 2 interface.

7.2.17.1 Command Syntax

`switchport vlan-stacking customer-edge-port (ethertype ETHERTYPE)`

`ETHERTYPE` Ethertype field for the vlan tag (in 0xhhhh hexadecimal notation).

7.2.17.2 Command Mode

Interface mode

7.2.17.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport vlan-stacking customer-edge-port ethertype 0x9100
```

7.2.18 switchport vlan-stacking provider-port ethertype VALUE

Use this command to enable VLAN stacking and set the switching characteristics of the Layer 2 interface to provider-edge port.

Use the no parameter to disable VLAN stacking of the Layer 2 interface.

7.2.18.1 Command Syntax

`switchport vlan-stacking provider-port (ethertype ETHERTYPE)`

ETHERTYPE Ethertype field for the vlan tag (in 0xhhhh hexadecimal notation).

7.2.18.2 Command Mode

Interface mode

7.2.18.3 Examples

```
# configure terminal
(config)# interface eth0
(config-if)# switchport vlan-stacking provider-port ethertype 0x9100
```

7.2.19 vlan bridge

This command enables or disables the state of a particular VLAN on a bridge basis. Specifying the disable state causes all forwarding over the specified VLAN ID on the specified bridge to cease. Specifying the enable state allows forwarding of frames on the specified VLAN-aware bridge.

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

7.2.19.1 Command Syntax

`vlan VLANID bridge <1-32> (name VLAN_NAME) (state [enable (intervlan-route [enable|disable])|disable])`

`no vlan VLANID bridge <1-32>`

`VLANID` The VID of the VLAN that will be enabled or disabled on the bridge <2-4022>.

`<1-32>` The ID of the bridge-group on which the VLAN will be affected.

`VLAN_NAME` The ASCII name of the VLAN. Maximum length: 16 characters.

`state enable` Sets VLAN into an enable state.

`state disable` Sets VLAN into a disable state.

`intervlan-route enable` Sets intervlan route into an enable state.

`intervlan-route disable` Sets intervlan route into a disable state.

The intervlan-route option is available only if the `state` is enabled.

If the intervlan-route is disabled, the packets from one VLAN will not be routed to another VLAN and the configured VLAN interface is not registered with the Operating System. As this is not an L3 interface, the interface properties, such as IP address, and MTU does not exist.

Conversely if the intervlan-route is enabled, VLAN interfaces are created in the Operating System as an L3 interface and hence the routing is in place.

7.2.19.2 Command Mode

VLAN Configuration mode

7.2.19.3 Examples

```
# configure terminal
(config)# vlan database
(config-vlan)# vlan 45 bridge 2 name vlan2 state enable intervlan-route enable
```

7.2.20 vlan classifier rule ipv4

Use this command to create an IPv4 subnet-based VLAN classifier rule and map it to a specific VLAN.

7.2.20.1 Command Syntax

`vlan classifier rule <1-256> ipv4 A.B.C.D/M vlan <2-4022>`

`no vlan classifier rule <1-256>`

`<1-256>` VLAN Classifier identifier

`A.B.C.D/M` IP Subnet

`<2-4022>` VLAN to which an untagged packet is mapped.

7.2.20.2 Command Mode

Configure mode

7.2.20.3 Usage

If the source IP address matches the IP subnet specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

7.2.20.4 Examples

```
# configure terminal
(config)# vlan classifier rule 3 ipv4 3.3.3.3/8 vlan 5
```

7.2.21 vlan classifier rule mac

Use this command to create a MAC address-based VLAN classifier rule, and map it to a specific VLAN.

Use the no parameter with this command to delete the specified VLAN classifier rule.

7.2.21.1 Command Syntax

`vlan classifier rule <1-256> mac WORD vlan <2-4022>`

`no vlan classifier rule <1-256>`

`<1-256>` VLAN classifier identifier

`WORD` Mac address

`<2-4022>` VLAN to which an untagged packet is mapped

7.2.21.2 Command Mode

Configure mode

7.2.21.3 Usage

If the source MAC address matches the MAC address specified in the VLAN classifier rule, the untagged received frames are mapped to the specified VLAN.

7.2.21.4 Examples

```
# configure terminal
(config)# vlan classifier rule 33 mac fe80::22e::b5ff:fee8:6/64 vlan 2
```

7.2.22 vlan classifier rule proto

Use this command to create a protocol type-based VLAN classifier rule, and map it to a specific VLAN.

7.2.22.1 Command Syntax

`vlan classifier rule <1-256> proto [ip|ipv6|<0-65535>|...] encap [ethv2|nosnapllc|snapllc] vlan <2-4022>`

`<1-256>` VLAN Classifier identifier

`proto` Type of protocol

encap Type of encapsulation

`<0-65535>` Other protocol values

`<2-4022>` VLAN to which an untagged packet is mapped

7.2.22.2 Command Mode

Configure mode

7.2.22.3 Usage

If the protocol type matches the protocol specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

7.2.22.4 Examples

```
# configure terminal
(config)# vlan classifier rule 34 proto ip encap ethv2 vlan 444
```

7.2.23 vlan database

Use this command to enter the VLAN configuration mode.

7.2.23.1 Command Syntax

`vlan database`

7.2.23.2 Command Mode

Configure mode

7.2.23.3 Usage

Use this command to enter the VLAN configuration mode, and add, delete, or modify values associated with a single VLAN.

7.2.23.4 Examples

In the following example, note the change to VLAN configuration mode from Configure mode:

```
# configure terminal
(config)# vlan database
(config-vlan)#
```

7.2.23.5 Related Commands

`vlan bridge`

7.2.24 vlan mtu bridge

Use this command to set the Maximum Transmission Unit (MTU) for a specified VLAN. Any packet with a size greater than the configured MTU is discarded.

Use the no parameter to reset the MTU configuration for the VLAN.

7.2.24.1 Command Syntax

`vlan VLANID mtu MTU_VALUE bridge BRIDGE_NAME`

`no vlan VLANID mtu bridge BRIDGE_NAME`

`VLANID` The ID of the VLAN for which the MTU has to be set.

`MTU_VALUE` The value of the Maximum Transmission Unit.

`BRIDGE_NAME` The name of the bridge on which VLAN is configured.

7.2.24.2 Command Mode

VLAN mode

7.2.24.3 Examples

```
(config-vlan)# vlan 2 mtu 1000 bridge 1
```

IGMP Snooping Commands

8.1 IGMP Commands

The Internet Group Management Protocol (IGMP) module includes the IGMP Proxy service and IGMP Snooping functionalities. Some of the following commands may have commonalities and restrictions: these are described under the Usage section for each command.

NOTE: This chapter is relevant, only if LAYER3SRS is licensed.

8.2 ip igmp snooping

Use this command to enable IGMP Snooping. When this command is given in the Global Config mode, IGMP Snooping is enabled at the switch level. When this command is given at the VLAN interface level, IGMP Snooping is enabled for that VLAN.

Use the no parameter with this command to globally disable IGMP Snooping, or for the specified interface.

8.2.1 Command Syntax

`ip igmp (vrf VRFNAME) snooping`

`no ip igmp (vrf VRFNAME) snooping`

`VRFNAME` Optional. Specify the VRF name.

8.2.2 Command Mode

Global Config mode
Interface mode for VLAN interface

8.2.3 Default

IGMP Snooping is enabled.

8.2.4 Usage

This IGMP Snooping command can only be configured on VLAN interfaces

8.2.5 Examples

```
# configure terminal
(config)# ip igmp snooping
(config)# interface vlan1.1
(config-if)# ip igmp snooping
```

8.3 ip igmp snooping fast-leave

Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the IGMP group-membership is removed, as soon as an IGMP leave group message is received without sending out a group-specific query.

Use the no parameter with this command to disable fast-leave processing.

8.3.1 Command Syntax

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

8.3.2 Command Mode

Interface mode for VLAN interface

8.3.3 Default

IGMP Snooping fast-leave processing is disabled.

8.3.4 Usage

This IGMP Snooping command can only be configured on VLAN interfaces.

8.3.5 Example

This example shows how to enable fast-leave processing on a VLAN.

```
# configure terminal
(config)# interface vlan1.1
(config-if)# ip igmp snooping fast-leave
```

8.4 ip igmp snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.

Use the no parameter with this command to remove the static configuration of the interface as a multicast router interface.

8.4.1 Command Syntax

`ip igmp snooping mrouter interface IFNAME`

`no ip igmp snooping mrouter interface IFNAME`

`IFNAME` Specify the name of the interface

8.4.2 Command Mode

Interface mode for VLAN interface

8.4.3 Usage

This IGMP Snooping command can only be configured on VLAN interfaces.

8.4.4 Example

This example shows interface fe8 statically configured to be a multicast router interface.

```
# configure terminal
(config)# interface vlan1.1
(config-if)# ip igmp snooping mrouter interface fe8
```

8.5 ip igmp snooping querier

Use this command to enable IGMP querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.

Use the no parameter with this command to disable IGMP querier configuration.

8.5.1 Command Syntax

```
ip igmp snooping querier
no ip igmp snooping querier
```

8.5.2 Command Mode

Interface mode for VLAN interface

8.5.3 Usage

This command can only be configured on VLAN interfaces.

The IGMP Snooping querier uses the 0.0.0.0 Source IP address because it only masquerades as a proxy IGMP querier for faster network convergence.

It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router.

It restarts as the IGMP Snooping querier if no queries are seen within the other querier interval.

8.5.4 Example

```
# configure terminal
(config)# interface vlan1.1
(config-if)# ip igmp snooping querier
```

8.6 ip igmp snooping report-suppression

Use this command to disable or enable snooping report suppression for IGMP versions 1 and 2 on VLAN interfaces.

Use the no parameter with this command to disable snooping report suppression (return snooping report suppression to its default state).

NOTE: This command does not apply to IGMPv3.

8.6.1 Command Syntax

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

8.6.2 Command Mode

Interface mode for VLAN interface

8.6.3 Default

Snooping report suppression is turned on (enabled) by default for IGMPv1 and IGMPv2 VLAN interfaces, and does not apply to IGMPv3.

8.6.4 Usage

IGMP snooping report suppression is for forwarding only one IGMP report per multicast router query to multicast devices. When IGMP snooping report suppression is enabled (the default setting), the switch only sends the first IGMP report from all hosts for a group to all multicast routers. The switch does not send the remaining IGMP reports for the group. This feature prevents duplicate reports from being sent to the multicast devices.

The enabling or disabling of IGMP report suppression can only be configured on VLAN interfaces.

8.6.5 Example

This example shows how to disable snooping report suppression for IGMPv2 reports:

```
# configure terminal
(config)# interface vlan1.1
(config-if)# ip igmp version 2
(config-if)# no ip igmp snooping report-suppression
```

This example shows how to enable snooping report suppression for IGMPv2 reports.

```
# configure terminal
(config)# interface vlan1.1
(config-if)# ip igmp version 2
(config-if)# ip igmp snooping report-suppression
```

8.7 ip igmp snooping last-leave

Use this command to enable snooping last leave for IGMPv2 on VLAN interfaces. Use the no parameter with this command to disable snooping last leave. By default last-leave is enabled.

NOTE: This command does not apply to IGMPv1 and IGMPv3.

8.7.1 Command Syntax

```
ip igmp snooping last-leave
no ip igmp snooping last-leave
```

8.7.2 Command Mode

Interface mode for VLAN interface

8.7.3 Default

Snooping last leave is turned on (enabled) by default for IGMPv2 VLAN interfaces, and does not apply to IGMPv1 and IGMPv3.

8.7.4 Usage

IGMP snooping last leave is for forwarding only one IGMP leave group report (type 0x17) to multicast router. When IGMP snooping last leave is enabled (the default setting), the snooping switch suppresses IGMP leave messages from IGMP hosts and does not forward them to the IGMP router as long as there is other active member hosts of the multicast group of interest onthe snooping switch.

The enabling or disabling of IGMP last leave can only be configured on VLAN interfaces.

8.7.5 Example

The following example shows how to disable snooping last leave for IGMPv2 leave reports:

```
#configure terminal
(config)#interface vlan2.5
(config-if)#ip igmp version 2
(config-if)#no ip igmp snooping last-leave
```

The following example shows how to enable snooping last leave for IGMPv2 leave reports:

```
#configure terminal
(config)#interface vlan2.5
(config-if)#ip igmp version 2
(config-if)#ip igmp snooping last-leave
```

8.8 show ip igmp snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token. For more information, see the *Chapter 1, Command Line Interface Environment*.

8.8.1 Command Syntax

`show ip igmp snooping mrouter interface IFNAME`

`IFNAME` The name of the VLAN interface

8.8.2 Command Mode

Exec and Privileged Exec mode

8.8.3 Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
# show ip igmp snooping mrouter vlan1.1
VLAN     Interface
1        ge9
1        ge11
```

8.9 show ip igmp snooping statistics

Use this command to display IGMP Snooping statistics data.

To modify the lines displayed, use the | (output modifier token). To save the output to a file, use the > output redirection token. For more information, see *Chapter 1, Command Line Interface Environment*.

8.9.1 Command Syntax

`show ip igmp snooping statistics interface IFNAME`

`IFNAME` The name of the VLAN interface

8.9.2 Command Mode

Exec and Privileged Exec mode

8.9.3 Example

The following displays IGMPv3 statistical information for bridge 2.

```
# show ip igmp snooping statistics interface vlan1.1
IGMP Snooping statistics for ge9
Interface:      ge10
Group:          225.0.0.1
Uptime:         00:00:09
Group mode:     Exclude (Expires: 00:04:10)
Last reporter:  4.4.4.5
Source list is empty
```

802.1x Commands

9.1 auth-mac auth-fail-action

Use this command to specify the required action after authentication fails for any source MAC (Media Access Control). If `drop-traffic` is specified, data destined to that MAC is dropped. The MAC will be added to the forwarding database in Discarded mode.

If `restrict-vlan` is specified, the unauthorized MAC is added to a restricted VLAN. The MAC will be added to the forwarding database in Forwarding mode.

9.1.1 Command Syntax

`auth-mac auth-fail-action [drop-traffic|restrict-vlan <2-4094>]`

9.1.2 Parameters

`drop-traffic` Drops traffic destined to unauthorized source.

`restrict-vlan` Adds unauthorized MAC address to restricted VLAN.

`<2-4094>` Range of values for VLAN ID.

9.1.3 Default

drop-traffic

9.1.4 Command Mode

Interface mode

9.1.5 Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac auth-fail-action restrict-vlan 12
```

9.2 auth-mac disable

Use this command to disable MAC authentication on a Carrier Ethernet interface. Refer to the auth mac enable command to enable MAC authentication on a Carrier Ethernet interface.

9.2.1 Command Syntax

`auth-mac disable [mode (filter|shutdown)]`

9.2.2 Parameters

`mode` Use this parameter to disable the MAC authentication mode on a Carrier Ethernet interface.

`filter` Filter the frames for the MAC when in an unauthorized state.

`shutdown` Shut down the interface when the MAC is unauthenticated.

9.2.3 Command Mode

Interface mode

9.2.4 Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac disable
#configure terminal
(config)#interface eth0
(config-if)#auth-mac disable mode filter
(config)#interface eth0
(config-if)#auth-mac disable mode shutdown
```

9.3 auth-mac dynamic-vlan-creation

Use this command to enable or disable dynamic VLAN creation after successful MAC authentication. If the user disables dynamic VLAN creation after a successful authentication, the MAC will be added to the forwarding database with the default VLAN. If the user enables dynamic VLAN creation after a successful authentication, the MAC under authentication will be added to the VLAN ID attribute in the radius server configuration-file.

9.3.1 Command Syntax

`auth-mac dynamic-vlan-creation [disable|enable]`

9.3.2 Parameters

`disable` Disable dynamic VLAN creation.

`enable` Enable dynamic VLAN creation.

9.3.3 Default

Disabled

9.3.4 Command Mode

Interface mode

9.3.5 Examples

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation disable
#configure terminal
(config)#interface eth0
(config-if)#auth-mac dynamic-vlan-creation enable
```

9.4 auth-mac enable

Use this command to enable MAC authentication on a Carrier Ethernet interface. Refer to the *auth-mac disable on page 181* command to disable MAC authentication on a Carrier Ethernet interface (see auth-mac disable).

9.4.1 Command Syntax

`auth-mac enable [mode (filter|shutdown)]`

9.4.2 Parameters

`mode` Use this parameter to enable the MAC authentication mode on a Carrier Ethernet interface.

`filter` Filter the frames for the MAC when in an unauthorized state.

`shutdown` Shut down the interface when the MAC is unauthenticated.

9.4.3 Command Mode

Interface mode

9.4.4 Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac enable
#configure terminal
(config)#interface eth0
(config-if)#auth-mac enable mode filter
(config)#interface eth0
(config-if)#auth-mac enable mode shutdown
```

9.5 auth-mac mac-aging

Use this command to enable or disable MAC aging. When enabled, a MAC entry is added to the forwarding database, with aging time equal to the bridge aging time. Otherwise, the MAC entry will not be aged out. If MAC aging is disabled, the MAC entry will not be aged out.

9.5.1 Command Syntax

`auth-mac mac-aging [enable|disable]`

9.5.2 Parameters

`disable` Disables MAC aging.

`enable` Enables MAC aging.

9.5.3 Command Mode

Interface mode

9.5.4 Example

```
#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging disable
#configure terminal
(config)#interface eth0
(config-if)#auth-mac mac-aging enable
```

9.6 auth-mac system-auth-ctrl

Use this command to enable MAC authentication globally. If MAC authentication is not enabled, other MAC authentication related commands throw an error when issued.

Use the no parameter with this command to disable MAC authentication globally.

9.6.1 Command Syntax

```
auth-mac system-auth-ctrl
no auth-mac system-auth-ctrl
```

9.6.2 Parameters

None

9.6.3 Command Mode

Configure mode

9.6.4 Examples

```
#configure terminal
(config)#auth-mac system-auth-ctrl
(config)#no auth-mac system-auth-ctrl
```

9.7 debug dot1x

Use this command to turn on or turn off 802.1x debugging at various levels.

Use the no parameter with this command to turn off debugging.

9.7.1 Command Syntax

```
debug dot1x [all|event|nsm|packet|timer]
no debug dot1x [all|event|nsm|packet|timer]
```

9.7.2 Parameters

`all` Set debugging for all 802.1x levels.

`event` Set debugging for 802.1x events.

`nsm` Set debugging for NSM information.

`packet` Set debugging for 802.1x packets.

`timer` Set debugging for 802.1x timer.

9.7.3 Command Mode

Exec, Privileged Exec, and Configure modes

9.7.4 Examples

```
#configure terminal
(config)#debug dot1x all
(config)#debug dot1x event
```

9.8 dot1x initialize

Use this command to remove authentication from a port, and attempt reauthentication on the specified interface.

9.8.1 Command Syntax

```
dot1x initialize [interface (IFNAME)]
```

9.8.2 Parameters

`IFNAME` Specify the interface name for debugging.

9.8.3 Command Mode

Privileged Exec

9.8.4 Examples

```
#dot1x initialize interface eth0
```

9.9 dot1x keytxenabled

Use this command to enable or disable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant.

9.9.1 Command Syntax

```
dot1x keytxenabled [disable|enable]
```

9.9.2 Parameters

`disable` Disables the key transmission.

`enable` Enables the key transmission.

9.9.3 Command Mode

Interface mode

9.9.4 Example

```
#configure terminal
(config)#interface eth0
(config-if) #dot1x keytxenabled disable
#configure terminal
(config)#interface eth0
(config-if) #dot1x keytxenabled enable
```

9.10 dot1x port-control

Use this command to force a port state.

Use the no parameter with this command to remove a port from the 802.1x management.

9.10.1 Command Syntax

```
dot1x port-control [auto]
dot1x port-control [dir (both|in)]
dot1x port-control [force-authorized]
dot1x port-control [force-unauthorized]
no dot1x port-control
```

9.10.2 Parameters

`auto` Specify to enable authentication on port.

`dir (both|in)` Specify the packet control direction.

`both` Discard receive and transmit packets from the supplicant

`in` Discard receive packets from the supplicant

`force-authorized` Specify to force a port to always be in an authorized state.

`force-unauthorized` Specify to force a port to always be in an unauthorized state.

9.10.3 Command Mode

Interface mode

9.10.4 Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x port-control auto
(config)#interface eth0
(config-if)#no dot1x port-control
```

9.11 dot1x protocol-version

Use this command to set the protocol version of dot1x to 1 or 2. The protocol version must be synchronized with the Xsupplicant being used in that interface.

Use the no parameter with this command to set the protocol version to the default value (2).

9.11.1 Command Syntax

```
dot1x protocol-version <1-2>
no dot1x protocol-version
```

9.11.2 Parameters

<1-2> Indicates the EAP Over LAN (EAPOL) version.

9.11.3 Default

The default dot1x protocol version is 2.

9.11.4 Command Mode

Interface mode

9.11.5 Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x protocol-version 2
(config)#interface eth0
(config-if)#no dot1x protocol-version
```

9.12 dot1x quiet-period

Use this command to set the quiet-period time interval.

When a switch cannot authenticate a client, the switch remains idle for a quiet-period interval of time, then tries again. By administratively changing the quiet-period interval, by entering a lower number than the default, a faster response time can be provided.

Use the no parameter with this command to set the configured quiet period to the default (60 seconds).

9.12.1 Command Syntax

```
dot1x quiet-period <1-65535>
no dot1x quiet-period
```

9.12.2 Parameter

<1-65535> Seconds between the retrial of authentication.

9.12.3 Default

The default dot1x quiet period is 60.

9.12.4 Command Mode

Interface mode

9.12.5 Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x quiet-period 200
```

9.13 dot1x reauthMax

Use this command to set the maximum reauthentication value, which sets the maximum number of reauthentication attempts after which the port will be unauthorized.

Use the no parameter with this command to set the reauthentication maximum to the default value (2).

9.13.1 Command Syntax

```
dot1x reauthMax <1-10>
no dot1x reauthMax
```

9.13.2 Parameter

<1-10> Indicates the maximum number of reauthentication attempts after which the port will be unauthorized.

9.13.3 Default

The default is 2.

9.13.4 Command Mode

Interface mode

9.13.5 Examples

The following sets the maximum reauthentication value to 5.

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthMax 5
```

The following sets the reauthentication maximum to the default value.

```
#configure terminal
(config)#interface eth0
(config-if)#no dot1x reauthMax
```

9.14 dot1x reauthentication

Use this command to enable reauthentication on a port.

Use the no parameter with this command to disable reauthentication on a port.

9.14.1 Command Syntax

```
dot1x reauthentication
no dot1x reauthentication
```

9.14.2 Parameters

None

9.14.3 Command Mode

Interface mode

9.14.4 Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x reauthentication
```

9.15 dot1x system-auth-ctrl

Use this command to enable global authentication.

Use the no parameter with this command to disable global authentication.

9.15.1 Command Syntax

```
dot1x system-auth-ctrl
no dot1x system-auth-ctrl
```

9.15.2 Parameters

None

9.15.3 Default

Authentication is off by default.

9.15.4 Command Mode

Configure mode

9.15.5 Example

```
#configure terminal
(config)#dot1x system-auth-ctrl
```

9.16 dot1x timeout re-authperiod

Use this command to set the interval between reauthorization attempts.

Use the no parameter with this command to disable the interval between reauthorization attempts.

9.16.1 Command Syntax

```
dot1x timeout re-authperiod <1-4294967295>
no dot1x timeout re-authperiod
```

9.16.2 Parameter

<1-4294967295> Specify the seconds between reauthorization attempts in the range of <1-4294967295>.

9.16.3 Default

Default time is 3600 seconds

9.16.4 Command Mode

Interface mode

9.16.5 Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout re-authperiod 25
```

9.17 dot1x timeout server-timeout

Use this command to set the authentication sever response timeout.

Use the no parameter with this command to disable the authentication sever response timeout.

9.17.1 Command Syntax

```
dot1x timeout server-timeout <1-65535>
no dot1x timeout server-timeout
```

9.17.2 Parameter

<1-65535> Specify the authentication server response timeout in the range of <1-65535>.

9.17.3 Default

Default timeout is 30 seconds.

9.17.4 Command Mode

Interface mode

9.17.5 Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout server-timeout 555
(config)#interface eth0
(config-if)#no dot1x timeout server-timeout
```

9.18 dot1x timeout supp-timeout

Use this command to set the interval for a supplicant to respond.

Use the no parameter with this command to disable the authentication sever response timeout.

9.18.1 Command Syntax

```
dot1x timeout supp-timeout <1-65535>
no dot1x timeout supp-timeout
```

9.18.2 Parameter

<1-65535> Specify the authentication server response timeout in the range of <1-65535>.

9.18.3 Default

Default timeout is 30 seconds.

9.18.4 Command Mode

Interface mode

9.18.5 Example

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout supp-timeout 40
(config)#interface eth0
(config-if)#no dot1x timeout supp-timeout
```

9.19 dot1x timeout tx-period

Use this command to set the interval between successive attempts to request an ID.

Use the no parameter to disable the interval between successive attempts to request an ID.

9.19.1 Command Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

9.19.2 Parameter

<1-65535> Specify the authentication server response timeout in the range of <1-65535>.

9.19.3 Default

Default timeout is 30 seconds.

9.19.4 Command Mode

Interface mode

9.19.5 Examples

```
#configure terminal
(config)#interface eth0
(config-if)#dot1x timeout tx-period 34
(config)#interface eth0
(config-if)#no dot1x timeout tx-period
```

9.20 ip radius source-interface

Use this command to set the local address sent in packets to the radius server.

Use the no parameter with this command to clear the local address.

9.20.1 Command Syntax

```
ip radius source-interface [HOSTNAME|PORT]
no ip radius source-interface
```

9.20.2 Parameters

HOSTNAME Specify the radius client in the dotted IP address, or in the hostname format.

PORT Specify the radius client port number. The default port number is 1812.

9.20.3 Command Mode

Configure mode

9.20.4 Examples

```
#configure terminal
(config)#ip radius source-interface myhost 1812
(config)#no ip radius source-interface myhost
```

9.21 radius-server deadtime

Use this command to specify the number of minutes a radius server, which is not responding to authentication requests, is passed over by requests for radius authentication. To improve radius response times when some servers might be unavailable, use this command to cause the unavailable servers to be skipped immediately.

Use the no parameter with this command to set deadtime to the default value of 0.

9.21.1 Command Syntax

```
radius-server deadtime [MIN <1-1440>]
no radius-server deadtime
```

9.21.2 Parameter

`MIN` Length of time (in minutes) that a radius server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours). Enter a value in the range 1 to 1440.

9.21.3 Default

Deadtime is set to 0

9.21.4 Command Mode

Configure mode

9.21.5 Examples

```
#configure terminal
(config)#radius-server deadtime 10
(config)#no radius-server deadtime
```

9.22 radius-server host

Use this command to specify the IP address or host name of the remote radius server host and assign authentication and accounting destination port numbers. Multiple radius-server host commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host.

If the auth-port parameter is not specified, it will take the default value of the auth-port. If you do not specify the authport to unconfigure, and the default value of the auth-port does not match the port you are trying to unconfigure, the specified radius-server host will not be unconfigured.

Use the no parameter with this command to unconfigure a specified radius-server.

9.22.1 Command Syntax

`radius-server host (HOSTNAME) [auth-port (PORTNO)|timeout (SEC <1-1000>)|retransmit (RETRIES <1-100>)|key (STRING)]`

`no radius-server host (HOSTNAME) [auth-port (PORTNO)]`

9.22.2 Parameters

`auth-port` (Optional) Specify the UDP destination port for authentication requests; the host is not used for authentication if set to 0.

`key` (Optional) Specify the authentication and encryption key for all radius communications between the router and the radius server. This key must match the encryption used on the radius daemon. All leading spaces are ignored, but spaces within and at the end of the string are used. If spaces are used in the string, do not enclose the string in quotation marks unless the quotation marks themselves are part of the key.

`retransmit` (Optional) The number of times a radius request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radiusserver retransmit command. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.

`timeout` (Optional) The time interval (in seconds) that the router waits for the radius server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.

9.22.3 Command Mode

Configure mode

9.22.4 Examples

```
#configure terminal
(config)#radius-server host 10.10.10.40 auth-port 1812 timeout 5
retransmit 3 key authd
(config)#no radius-server host 10.10.10.40 auth-port 1812
```

9.23 radius-server key

Use this command to set the shared secret key between a Radius server and a client.

Use the no parameter with this command to undo this configuration.

9.23.1 Command Syntax

```
radius-server key [KEY]
no radius-server key
```

9.23.2 Parameter

KEY Specify the secret key shared among the radius server and the 802.1x client.

9.23.3 Command Mode

Configure mode

9.23.4 Examples

```
#configure terminal
(config)#radius-server key ipi
#configure terminal
(config)#no radius-server key
```

9.24 radius-server retransmit

Use this command to specify the number of times the router transmits each radius request to the server before giving up.

Use the no parameter with this command to disable retransmission.

9.24.1 Command Syntax

```
radius-server retransmit [RETRIES <1-100>]
no radius-server retransmit
```

9.24.2 Parameter

RETRIES Specify the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.

9.24.3 Default

The default value is 3.

9.24.4 Command Mode

Configure mode

9.24.5 Examples

```
#configure terminal
(config)#radius-server retransmit 12
(config)#no radius-server retransmit
```

9.25 radius-server timeout

Use this command to specify the number of seconds a router waits for a reply to a radius request before retransmitting the request.

Use the no parameter with this command to use the default value.

9.25.1 Command Syntax

```
radius-server timeout (SEC <1-1000>)
no radius-server timeout
```

9.25.2 Parameter

SEC The number of seconds for a router to wait for a server host to reply before timing out. Enter a value in the range 1 to 1000.

9.25.3 Default

The default value is 5 seconds.

9.25.4 Command Mode

Configure mode

9.25.5 Examples

```
#configure terminal
(config)#radius-server timeout 20
#configure terminal
(config)#no radius-server timeout
```

9.26 show debugging dot1x

Use this command to display the status of the debugging of the 802.1x system.

9.26.1 Command Syntax

```
show debugging dot1x
```

9.26.2 Parameters

None

9.26.3 Command Mode

Privileged Exec mode

9.26.4 Example

```
#show debugging dot1x
802.1X debugging status
```

9.27 show dot1x

Use this command to display the state of the whole system.

9.27.1 Command Syntax

```
show dot1x [all]
```

```
show dot1x [diagnostics interface (IFNAME)]
show dot1x [interface (IFNAME)]
show dot1x [sessionstatistics interface (IFNAME)]
show dot1x [statistics interface (IFNAME)]
```

9.27.2 Parameters

`all` Display all information.

`diagnostics` Display diagnostics information.

`IFNAME` Display diagnostics information for this interface.

`interface` Display interface information.

`sessionstatistics` Display session statistics.

`IFNAME` Display session statistics information for this interface.

`statistics` Display statistics information.

`IFNAME` Display statistics information for this interface.

9.27.3 Command Mode

Exec mode and Privileged Exec mode

9.27.4 Displayed Output

The following tables describes the output for the show dot1x all command and the show dot1x interface command.

Table 9-1 Output for show dot1x all Command

Entry	Description
portEnabled	Interface operational status (Up-true/down-false)
portControl	Current control status of the port for 802.1x control
portStatus	802.1x status of the port (authorized/unauthorized)
reAuthenticate	Reauthentication enabled/disabled status on port
reAuthPeriod	Value holds meaning only if reAuthentication is enabled

Table 9-2 Supplicant PAE related global variables

Entry	Description
abort	Indicates that authentication should be aborted when set to true
fail	Indicates failed authentication attempt when set to false
start	Indicates authentication should be started when set to true
timeout	Indicates authentication attempt timed out when set to true
success	Indicates authentication successful when set to true

Table 9-3 Current 802.1x Operational State of Interface

Entry	Description
mode	Configured 802.1x mode
reAuthCount	Reauthentication count
quietperiod	Time between reauthentication attempts
reAuthMax	Maximum reauthentication attempts

Table 9-4 Backend Authentication state machine variables and constants

Entry	Description
state	State of the state machine
reqCount	Count of requests sent to server
suppTimeout	Supplicant timeout
serverTimeout	Server timeout
maxReq	Maximum requests to be sent

Table 9-5 Controlled Directions State machine

Entry	Description
adminControlledDirections	Administrative value (Both/In)

Table 9-5 Controlled Directions State machine (continued)

Entry	Description
operControlledDirections	Operational Value (Both/In)

Table 9-6 KR -- Key receive state machine

Entry	Description
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted

Table 9-7 Key Transmit State machine

Entry	Description
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange
keyTxEnabled	Key transmission enabled/disabled status

9.27.5 Example

The following is an output of this command displaying the state of the system:

```
#show dot1x
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.ipinfusion.com.12103
% Next radius message id: 0
```

The following is an output of this command displaying detailed information for all ports.

```
#show dot1x all
% 802.1x authentication enabled
% Radius server address: 192.168.1.1.1812
% Radius client address: dhcp128.ipinfusion.com.12103
% Next radius message id: 0
% Dot1x info for interface eth1 - 3
% portEnabled: true - portControl: auto
% portStatus: unauthorized - currentId: 11
% reAuthenticate: disabled
```

```
% abort:F fail:F start:F timeout:F success:F
% PAE: state: connecting - portMode: auto
% PAE: reAuthCount: 2 - rxRespId: 0
% PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
% BE: state: idle - reqCount: 0 - idFromServer: 0
% BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
% CD: adminControlledDirections: in - operControlledDirections: in
% CD: bridgeDetected: false
% KR: rxKey: false
% KT: keyAvailable: false - keyTxEnabled: false
```

Related Documentation

A.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 A-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 Configuration Guide	6806800N86
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