PENGUIN™
SOLUTIONS

SRstackware® Intelligent Network Software

Switch Configuration Command Reference

P/N: 6806800N92V

August 2022

PENGUIN™
EDGE

Legal Disclaimer*

SMART Embedded Computing, Inc. (SMART EC), dba Penguin Solutions™, 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 The text itself may not be published commercially in print or electronic form, edited, translated, or otherwise altered without the permission of SMART EC.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 EC.

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., dba Penguin Solutions

2900 S. Diablo Way, Suite 190

Tempe, Arizona 85282

USA

*For full legal terms and conditions, visit *https://www.penguinsolutions.com/edge/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® IP routing software should use this Command Reference.

This document contains the following chapters:

SRstackware provides Telnet services so that users can log into any of the routing module layers and control the module by using the Command Line Interface (CLI).

Abbreviations

This document uses the following abbreviations:

Abbreviation	Definition
ACL	Access Control List
ARS	Advanced Routing Suite
AS	Autonomous System
CLI	Command Line Interface
CoS	Class of Service
DSCP	Differentiated Services Code Point
FIB	Forwarding Information Base

Abbreviation	Definition
IGP	Interior Gateway Protocol
IPMC	Intelligent Platform Management Controller
LSA	Link State Advertisement
MPLS	Multi-protocol Label Switching
MTU	Maximum Transmission Unit
NSM	Network Services Module
QoS	Quality of Service
SNMP	Simple Network Management Protocol
SRstackware	Switching and Routing stackware
TTL	Time to Live
UDF	User Defined Fields
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin

Conventions

The following table describes the conventions used throughout this manual.

Notation	Description
0x00000000	Typical notation for hexadecimal numbers (digits are 0 through F), for example used for addresses and offsets
0b0000	Same for binary numbers (digits are 0 and 1)
bold	Used to emphasize a word
`Screen`	Used for on-screen output and code related elements or commands. `Sample of Programming used in a table (9pt)`
`Courier + Bold`	Used to characterize user input and to separate it from system output
Reference	Used for references and for table and figure descriptions
File > Exit	Notation for selecting a submenu
<text>	Notation for variables and keys
[text]	Notation for software buttons to click on the screen and parameter description
...	Repeated item for example node 1, node 2, ..., node 12

Notation	Description
. . .	Omission of information from example/command that is not necessary at the time
..	Ranges, for example: 0..4 means one of the integers 0,1,2,3, and 4 (used in registers)
|	Logical OR
	Indicates a hazardous situation which, if not avoided, could result in death or serious injury
	Indicates a hazardous situation which, if not avoided, may result in minor or moderate injury
	Indicates a property damage message
	Indicates a hot surface that could result in moderate or serious injury
	Indicates an electrical situation that could result in moderate injury or death
	Indicates that when working in an ESD environment care should be taken to use proper ESD practices
	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
6806800N92V	August 2022	Rebrand to Penguin Solutions.
6806800N92U	March 2020	Rebrand to SMART Embedded Computing template
6806800N92T	December 2017	Updated copyrights page.
6806800N92S	July 2017	Added registered trademark to SRstackware.
6806800N92R	December 2016	Updated *clear counters on page 58*. Re-branded to new template.
6806800N92P	April 2016	Added a Notice in the Chapter 2, mirror interface, on page 103, Added *paired-link on page 124 and show paired-links on page 156.*
6806800N92N	February 2015	Added UDF and Range Checker commands in the Chapter 3, Matchlist Commands, on page 173. Updated Chapter 2, ip-access-group, on page 82.
6806800N92M	October 2014	Updated Appendix B, Rx/Tx Drop Counters, on page 309.
6806800N92L	October 2014	Added a note in description on page 69 and Appendix C, SRS Fixed MAC Address Implementation, on page 313.
6806800N92K	August 2014	Added show flowcontrol on page 139. Updated mirror interface on page 103.
6806800N92J	July 2014	Added Chapter 4, VLAN match-list Commands, on page 195 and Chapter 5, Egress match-list, on page 205. Updated Appendix B, Rx/Tx Drop Counters, on page 309.
6806800N92H	June 2014	Added clear running-config on page 65, log real-time on page 91 and match-list-priority on page 176. Updated show statistics on page 159, show statistics interface IFNAME drop-counters on page 161, show statistics vlan VLAN-ID on page 162, show storm-control on page 163, and match-list on page 173. Re-branded to Artesyn template.
6806800N92G	December 2013	Updated police on page 228.
6806800N92F	November 2013	Added ip-access-group on page 82.

Part Number	Publication Date	Description
6806800N92E	October 2013	Added show statistics interface IFNAME drop-counters on page 161, show statistics vlan VLAN-ID on page 162, clear counters vlan VLAN-ID on page 64, and Appendix B, Rx/Tx Drop Counters, on page 309.
6806800N92D	September 2013	Removed mac-address-limit, mac-address-limit vlan, and show mac-address-limit commands, as the Switch device on ATCA-F140 does not support MAC Address Limiting feature.
6806800N92C	April 2013	Added mac-learning on page 96. Updated match l3param on page 178.
6806800N92B	October 2012	Added mac-address-limit, mac-address-limit vlan, and show mac-address-limit.
6806800N92A	February 2012	Initial Release

SRstackware CLI 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 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. Only one user is allowed to use the Configure mode at a time.

The Integrated Management Interface (IMI) Shell gives users and administrators the ability to issue commands to several daemons from a single telnet session.

1.1.1 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 and 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 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 partial spelling of the command or parameter is ambiguous, then 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 commands that start with letter i, such as `interface`, `ip`, and `isis`. 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. For more information on the output modifiers and output redirection, see the Special Tokens for Show Commands section.

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.

Table 1-1 Typographic Conventions

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`**]**

Table 1-1 Typographic Conventions (continued)

Convention	Name	Description	Example
?	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)
< >	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. .

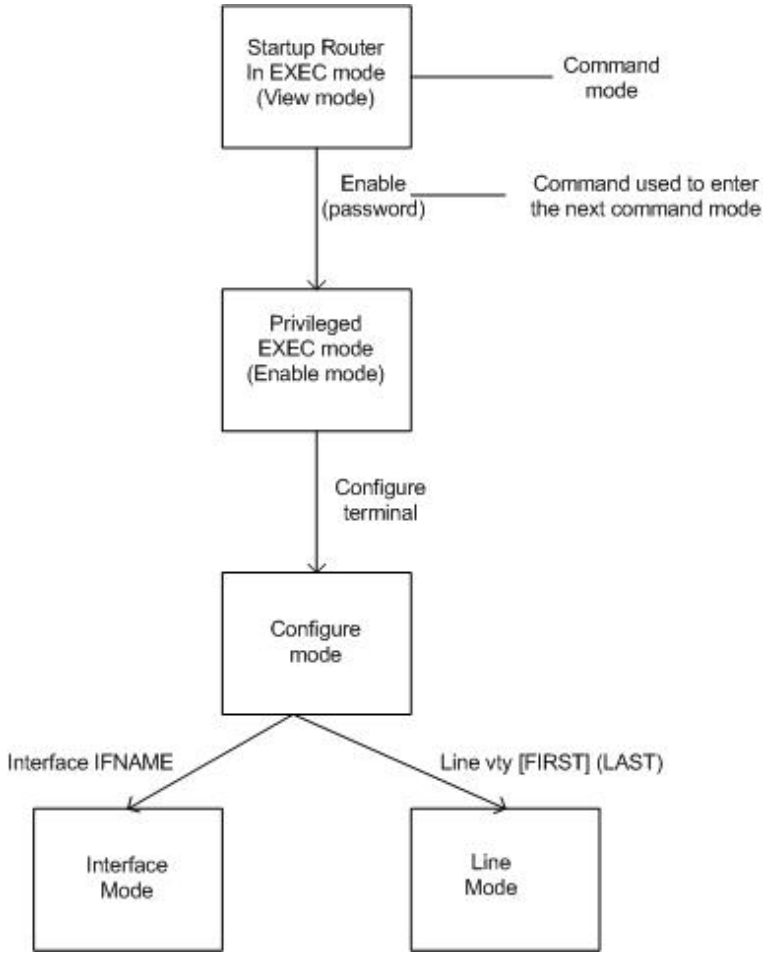
Multiple users can telnet and issue commands using the Exec mode and the Privileged Exec mode. Only one user is allowed to use the Configure mode at a time.

Table 1-2 Common Command Modes Descriptions

Mode	Description
Exec	Also called the View mode, is the base mode from where users can perform basic commands like `show`, `exit`, `quit`, `help`, `list`, and `enable`. All SRstackware daemons have this mode.
Privileged Exec	Also called the Enable mode, allows users to run `debug`, `write` (for saving and viewing the configuration) and `show` commands
Configure	Also called Configure Terminal mode, this mode serves as a gateway into the `Interface, Router, Line, Route Map, Key Chain` and `Address Family` modes.
Interface	Used to configure protocol-specific settings for a particular interface. Any attribute configured in this mode overrides an attribute configured in the `Router` mode
Line	Makes the `access-class` commands available

The diagram below displays the common command mode tree.

Figure 1-1 Command Mode Tree



1.6 QoS Command Modes

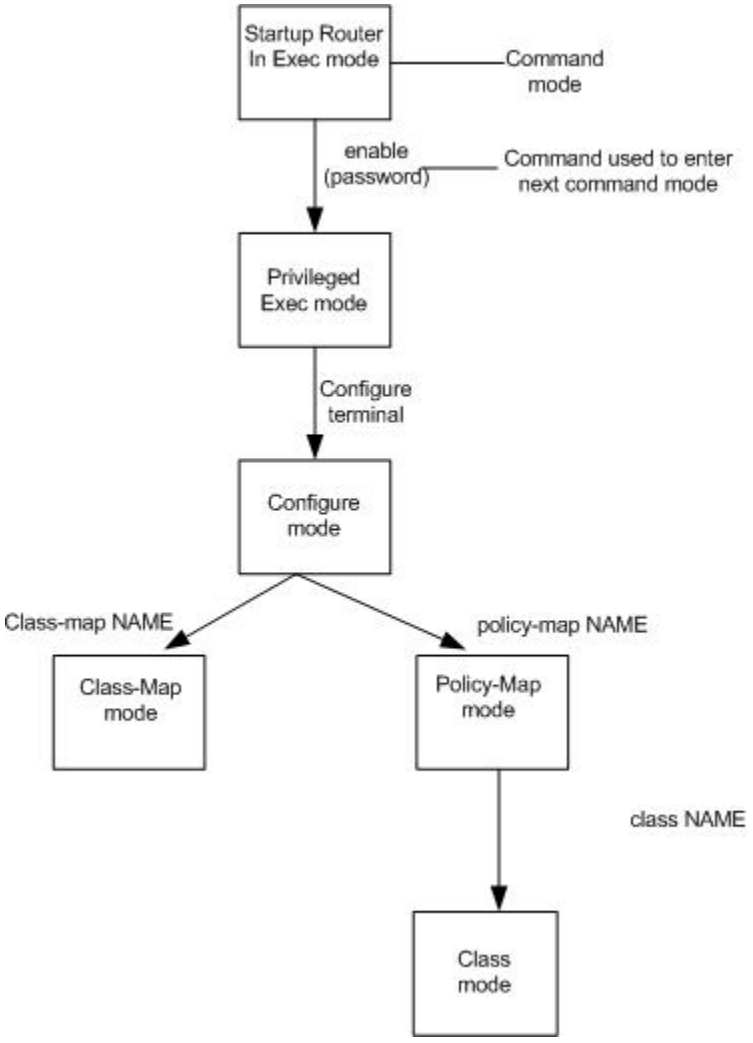
Class Map: Use this mode to create class maps. A class map names and isolates specific traffic from other traffic, and defines criteria to match against a specific traffic flow to further classify it.

Policy Map: Use this mode to create policy maps. A policy map specifies on which traffic class to act.

Class: Use this mode to define a traffic classification.

The following figure shows the complete QoS module command mode tree. For information about Exec, Privileged Exec, Configure and Interface modes, refer to the NSM daemon command modes mentioned earlier in this chapter.

Figure 1-2 QoS Command Mode Tree



Commands Common to Multiple Protocols

2.1 access-list

Use the `access-list` command to configure an access list for filtering packets. Use the `no` parameter to remove a specified access-list.

2.1.1 Command Syntax

`(no) access-list LISTNAME (DENY|PERMIT|REMARK)`

`LISTNAME = WORD DENY|PERMIT|REMARK =` IP SRstackware access-list

`DENY = deny [A.B.C.D/M (exact-match)]|any =` Specify route to reject

`PERMIT = permit [A.B.C.D/M (exact-match)]|any =` Specify route to permit

`A.B.C.D =` An IP address

`M =` Mask specifying which part of the IP address will be ignored

`any =` Allows any IP address or prefix to match

`exact-match =` Specifies exact matching of prefixes

`REMARK = remark .LINE`

`LINE =` Multi-line, access-list entry comment up to 100 characters

2.1.2 Command Mode

Configure mode

2.1.3 Usage

Use access lists to control the transmission of packets on an interface, and restrict contents of routing updates. The switch stops checking the access list after a match occurs.

When using this command from a Telnet session, be sure to telnet to the relevant protocol daemon (for example, isisd); unpredictable results can occur if this command is used in a telnet session with the NSM daemon.

2.1.4 Examples

```
# configure terminal
(config)# access-list mylist deny 10.10.0.72/24 exact-match
(config)# access-list mylist permit any
```

2.1.5 Validation Commands

`show running-config, show ip access-list, show ipv6 access-list`

For sample output of the validation commands, refer to Appendix A, *access-lists on page 231*.

2.2 access-list extended

Use the `access-list extended` command to configure an access list for filtering packets. Use the `no` parameter to remove a specified access-list.

2.2.1 Command Syntax

`(no) access-list EXTENDED (deny|permit|REMARK)ip SOURCE DESTINATION`

`(no) access-list EXTENDED (deny|permit|REMARK)ip any any`

`EXTENDED = <100-199>|<2000-2699>`

`<100-199> =` IP extended access list

`<2000-2699> =` IP extended access list (expanded range)

`deny =` Specify route to reject

`permit =` Specify route to permit

`REMARK = remark .LINE`

`LINE =` Multi-line, access-list entry comment up to 100 characters

`SOURCE = [A.B.C.D WILDCARDS]|any|[host A.B.C.D]`

`A.B.C.D =` IP address of the Source

`WILDCARD =` Wildcard mask to specify which part of A.B.C.D are ignored. It works as a reverse address mask, e.g., 0.0.0.255 means you permit or deny the route which matches the first 24 bits, A.B.C.D.

`DESTINATION = [A.B.C.D WILDCARDS]|any|[host A.B.C.D]`

`A.B.C.D` = IP address of the Destination

`WILDCARD` = Wildcard mask to specify which part of A.B.C.D is ignored. It works as a reverse address mask, e.g., 0.0.0.255 means you permit or deny the route which matches the first 24 bits, A.B.C.D.

`any` = Allows any IP address or prefix to match

`host` = Host A.B.C.D. A single host address

2.2.2 Command Mode

Configure mode

2.2.3 Usage

When using this command from a Telnet session, be sure to telnet to the relevant protocol daemon (for example, isisd); unpredictable results can occur if this command is used in a telnet session with the NSM daemon.

2.2.4 Examples

```
# configure terminal
(config)# access-list 134 deny ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255
(config)# access-list 2345 permit ip host 10.10.2.76 host 20.20.2.70
```

2.2.5 Validation Commands

`show running-config, show ip access-list, show ipv6 access-list`

For sample output of the validation commands, refer to Appendix A, *access-list extended on page 234*.

2.3 access-list standard

Use the `access-list standard` command to configure an access list for filtering packets. Use the `no` parameter to remove a specified access-list.

2.3.1 Command Syntax

(no) access-list STANDARD (DENY|PERMIT|REMARK)

STANDARD = <1-99>|<1300-1999>

<1-99> = IP standard access list

<1300-1999> = IP standard access list (expanded range)

DENY = deny [A.B.C.D (WILDCARD)]|any|host = Specify route to reject

PERMIT = permit [A.B.C.D (WILDCARD)]|any|host = Specify route to permit

A.B.C.D = An IP address

WILDCARD = wildcard mask to specify which part of A.B.C.D is ignored. It works as a reverse address mask, e.g., 0.0.0.255 means you permit or deny the route which matches the first 24 bits, A.B.C.D.

any = Allows any IP address or prefix to match

host = host A.B.C.D. A single host address

REMARK = remark .LINE

LINE = Multi-line, access-list entry comment up to 100 characters

2.3.2 Command Mode

Configure mode

2.3.3 Usage

When using this command from a Telnet session, be sure to telnet to the relevant protocol daemon (for example, isisd); unpredictable results can occur if this command is used in a telnet session with the NSM daemon.

2.3.4 Examples

```
# configure terminal
(config)# access-list 67 deny 1.1.1.0 0.0.0.255
(config)# access-list 1332 permit any
```

2.3.5 Validation Commands

`show running-config, show ip access-list, show ipv6 access-list`

For sample output of the validation commands, refer Appendix A, *access-list standard on page 237*.

2.4 bandwidth

Use this command to specify the maximum bandwidth to be used for each interface for duplex full/half mode. The bandwidth value is in bits, and can also accept units. This command must not be used on aggregator interfaces. Use the no parameter to remove the maximum bandwidth.

Set the duplex mode of the interface to "duplex full/half" before setting the bandwidth.

2.4.1 Command Syntax

`(no) bandwidth BANDWIDTH`

`BANDWIDTH`

`<1-999> = k|m for 1 to 999 kilo bits or mega bits`

`<1-10> = g for 1 to 10 giga bits`

2.4.2 Command Mode

Interface mode

2.4.3 Examples

```
# configure terminal
(config)# interface eth0
(Config-if)#shutdown
(Config-if)#duplex full
(Config-if)#bandwidth 1g
(Config-if)#no shutdown
```

2.4.4 Related Commands

`reservable-bandwidth`

2.4.5 Validation Commands

`show running-config, show interface`

For sample output of the validation commands, refer to Appendix A, *bandwidth on page 239*.

2.5 clear counters

Use this command to clear VLAN or interface counter statistics. Clearing counters not supported for Inter-Vlan interfaces.

2.5.1 Command Syntax

```
clear counters (IFNAME | all | vlan <VLAN_ID>)
  IFNAME   Interface or comma separated list of interfaces or range
           of Interfaces separated by -
  all      All interfaces
  vlan     clear counters for a particular vlan
  <2-4022> VLAN id
```

2.5.2 Command Mode

Exec mode and Privileged Exec mode

2.5.3 Example

```
#clear counters vlan 91
#clear counters all
#clear counters ge1
```

2.6 clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries.

2.6.1 Command Syntax

`clear ip prefix-list (WORD) (A.B.C.D/M)`

`WORD` = Specify the name of the prefix-list

`A.B.C.D/M` = IP prefix and length

2.6.2 Command Mode

Privileged Exec mode

2.6.3 Examples

```
# clear ip prefix-list List1
```

2.7 clear running-config

Use this command to clear various types of system configurations. Currently, this command does not clear all configurations. Configurations listed under *Section 2.7.3, Examples on page 60* are the only commands that can be cleared.

2.7.1 Command Syntax

`clear running-conifg (all | bridge |vlan | port | trunk | match-list)`

Command	Description
`Clear all`	clears entire configuration related to bridge, vlan, port, trunk and match-list.
`Clear bridge`	Clears configuration related to bridge, vlan and some port related configuration.
`Clear vlan`	clears entire vlan configuration including interface mode vlan configuration.
`Clear port`	Clears switch configuration in interface mode.
`Clear trunk`	Clears static-channel and channel-group configurations.
`Clear match-list`	Clears all match-list related configuration.

2.7.2 Command Mode

Configuration mode

2.7.3 Examples

```
(config)#clear running-config all
```

Examples of related commands which will be cleared during clear running-config:

- CLIs cleared during bridge clear

```
Config and vlan mode commands:
bridge 1 protocol ieee vlan-bridge
vlan 100 bridge 1 state enable
bridge-group 2 spanning-tree disable
paired-link ge1 ge2

Interface mode commands:
switchport mode hybrid
switchport hybrid vlan 92
switchport mode hybrid acceptable-frame-type all
switchport hybrid allowed vlan add 92 egress-tagged disable
switchport mode hybrid ingress-filter enable
switchport vlan-stacking provider-port
storm-control dlf level 20
```

- CLIs cleared during port clear in interface mode

```
flowcontrol both
mtu 1600
mac-learning disable
```

- CLIS which will be cleared during vlan clear

```
vlan 100 bridge 1 state enable
switchport hybrid vlan 92
switchport hybrid allowed vlan add 92 egress-tagged disable
```

- CLIs cleared during trunk clear

```
During this cleanup "sa" and "po" port will be deleted
interface sa1
port-channel load-balance src-dst-mac
interface po1
port-channel load-balance src-dst-mac
```

- CLIs cleared during match-list clear
  ```
  match-list 2035 fabric
  match l3param protocolid 112
  rule match-list 2010 action modify-IntPriority 7
  ```

2.8 configure terminal

Use the `configure terminal` command to enter the `Configure` command mode.

2.8.1 Command Syntax

```
configure terminal
```

2.8.2 Command Mode

Privileged Exec mode

2.8.3 Examples

The following example shows the use of the `configure terminal` command to enter the Configure command mode (note the change in the command prompt).

```
# configure terminal
(config)#
```

2.9 copy running-config startup-config

Use the `copy running-config startup-config` to write configurations to the file to be used at startup. This is the same as the write memory command.

2.9.1 Command Syntax

```
copy running-config startup-config
```

2.9.2 Command Mode

Privileged Exec mode

2.9.3 Examples

```
# copy running-config startup-config
```

2.10 description

Use this command to provide an interface-specific description.

NOTICE

The ATCA-F140 Fabric interfaces can be configured in group mode or independent mode. To reflect the port mode and bandwidth, the description command is updated by SRStackware during boot.

Due to this, the description command does not support persistency. If you want to set the description, you need to configure it after every boot once system stables, which takes around 50-60 seconds.

2.10.1 Command Syntax

`description .LINE`

`LINE` = Characters describing the specific interface.

2.10.2 Command Mode

Interface mode

2.10.3 Usage

This command is used to provide description about a particular interface.

2.10.4 Examples

The following example provides information about the connecting router for interface `eth1`.

```
Router# configure terminal
Router(config)# interface eth1
Router(config-if)# description Connected to Zenith's fas2/0
```

2.10.5 Validation Commands

`show running-config`

2.11 disable

Use the `disable` command to exit from the Privileged Exec mode, and return to the Exec mode.

2.11.1 Command Syntax

`disable`

2.11.2 Command Mode

Privileged Exec mode

2.11.3 Usage

This is the only command that allows user to go back to the Exec mode. Using the `exit` or `quit` command from the Privileged Exec mode ends the session, instead of going back

2.11.4 Examples

```
# disable
>
```

2.11.5 Related Commands

`enable, end, exit`

2.12 duplex

Use this command to set the data transmission mode of the interface. The configured bandwidth value is not considered when duplex is set to auto. This command must not be used on aggregator interfaces. Set the duplex mode as follows:

1. shutdown the port
2. set the duplex mode

3. If duplex mode is auto, reset the bandwidth else set bandwidth appropriately
4. no shutdown the port

2.12.1 Command Syntax

`duplex (auto|full|half)`

`auto` = Set the interface in the autonegotiation mode

`full` = Set the interface in the full duplex mode

`half` = Set the interface in the half duplex mode

2.12.2 Command Mode

Interface mode

2.12.3 Example

Duplex auto configuration:

```
# configure terminal
(config)# interface ge1
(Config-if)# shutdown
(Config-if)# duplex auto
(Config-if)#no bandwidth
(Config-if)#no shutdown
```

Duplex Full/half configuration:

```
(config)# interface ge1
(Config-if)#shutdown
(Config-if)#duplex full
(Config-if)#bandwidth 1g
(Config-if)#no shutdown
```

2.12.4 Validation Commands

`show interface, show running-config interface`

For sample output of the validation commands, refer Appendix A, *duplex on page 242*.

2.12.5 Related commands

`bandwidth`

2.13 enable

Use the `enable` command to enter the Privileged Exec command mode.

2.13.1 Command Syntax

`enable`

2.13.2 Command Mode

Exec mode

2.13.3 Usage

To return to the Exec mode from Privileged Exec mode, use the disable command. Using the `exit` or `quit` command from Privileged Exec mode ends the session.

2.13.4 Examples

The following example shows the use of the `enable` command to enter the Privileged Exec mode (note the change in the command prompt).

```
> enable
#
```

2.13.5 Related Commands

`disable, exit, quit`

2.14 end

Use the `end` command to return to the Privileged Exec command mode from any other advanced command mode.

2.14.1 Command Syntax

end

2.14.2 Command Mode

All command modes

2.14.3 Examples

The following example shows the use of the `end` command to return to the Privileged Exec mode directly from Interface mode.

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

2.14.4 Related Commands

`exit, disable, enable`

2.15 exec-timeout

Use the `exec-timeout` command to set the interval the command interpreter waits for user input detected. Use the **no** parameter to disable the wait interval.

2.15.1 Command Syntax

`exec-timeout MINUTES (SECONDS)`

`no exec-timeout`

`MINUTES = <0-35791> =` Timeout value in minutes

`SECONDS = <0-2147483> =` Timeout value in seconds

2.15.2 Command Mode

Line mode

2.15.3 Usage

This command is used to set the time for telnet session, which waits for an idle VTY session before it times out. An `exec-timeout 0 0` setting will cause the telnet session to wait indefinitely.

2.15.4 Examples

In the following example, the telnet session will time out after 2 minutes, 30 seconds if there is no response from the user.

```
Router# configure terminal
Router(config)# line vty 23 66
Router(config-line)# exec-timeout 2 30
```

2.15.5 Validation Commands

```
show running-config
```

2.16 exit

Use the `exit` command to exit from the current mode, and return to the previous level. When used in `Exec` mode, the `exit` command terminates the session.

2.16.1 Command Syntax

```
exit
```

2.16.2 Command Mode

All command modes

2.16.3 Examples

The following example shows the use of `exit` command to exit Interface mode, and return to Configure mode.

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

2.16.4 Related Commands

`end, enable, disable`

2.17 fib retain

Use this command to modify the retain time for stale routes in the Forwarding Information Base (FIB) during NSM restart.

Use the `no` parameter with this command to revert to default; not retaining NSM routes in the FIB when NSM is killed.

NSM still retains the stale routes for 60 seconds when it restarts.

2.17.1 Command Syntax

`(no) fib retain (TIME|Forever)`

`Forever Specifies an infinite retain time for stale routes.`

`TIME = time <1-65535> Specifies the retain time for stale routes. The default retain time is 60 seconds.`

`<1-65535> The retain time in seconds.`

2.17.2 Default

NSM routes are cleared from the FIB when NSM is killed, but when NSM is restarted, stale routes are retained for 60 seconds.

2.17.3 Command Mode

Configure mode

2.17.4 Usage

NSM reads the FIB and treats previously self-installed routes as stale routes. You can display stale routes by running the `show ip route database` command. All routes preceded by the symbol `p` are stale routes. When protocol modules restart, NSM overrides these stale routes with routes reinstalled by protocol modules.

The behavior of NSM routes when NSM is killed is as follows:

- no fib retain (default) Cleans up NSM routes from the FIB, but retains stale routes for 60 seconds when restarted.

- fib retain does not clear routes from the FIB, and retains stale routes for 60 seconds when restarted.
- fib retain forever does not clear routes from the FIB and retains stale routes forever.
- fib retain time <1-65535> does not clear routes from the FIB and retains stale routes for the specified seconds.

You can remove stale routes at any time by using the `clear ip route kernel` command.

2.17.5 Examples

```
# configure terminal
(config)# fib retain time 180
```

2.18 flowcontrol off

Use this command to disable flow control.

2.18.1 Command Syntax

`flowcontrol [send|receive] off`

`send` = Disables the flow control mode from sending

`receive` = Disables the flow control mode from receiving

2.18.2 Command Mode

Interface mode

2.18.3 Example

```
# configure terminal
(config)# interface eth1
(config-if)# flowcontrol receive off
```

2.19 flowcontrol on

Use this command to enable flow control, and configure the flow control mode for the port.

2.19.1 Command Syntax

`flowcontrol [send|receive] on`

`send` = Sets the port flow control mode to sending

`receive` = Sets the port flow control mode for receiving

2.19.2 Command Mode

Interface mode

2.19.3 Usage

Flow control enables connected Ethernet ports to control traffic rates during periods of congestion by allowing congested nodes to pause link operations at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When a local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the period of congestion.

2.19.4 Example

```
# configure terminal
(config)# interface eth0
(config-if)# flowcontrol send on
```

2.20 help

Use the `help` command to display a description of the SRstackware help system.

2.20.1 Command Syntax

`help`

2.20.2 Command Mode

All command modes

2.20.3 Usage

This is the sample output from the `help` command:

```
# help
SRstackware VTY provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
 until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show me?'.)
```

2.20.4 Examples

```
# configure terminal
(config)# help
```

2.21 hostname

Use the `hostname` command to set or change the network server name. SRstackware daemons use this name in system prompts and default configuration file names. Use the `no` parameter to disable this function.

When using the `hostname` command through IMISH, you must write to memory using the `write memory` or `write file` command. If you have not written to memory, the change made by this command (the new hostname) is not available when you log into IMISH the next time.

2.21.1 Command Syntax

`(no) hostname HOSTNAME`

`HOSTNAME` = Specifies the network name of the system

2.21.2 Command Mode

Configure mode

2.21.3 Usage

This command provides a hostname for login purposes only, and not for the enable mode. A hostname could be added for each remote system with which the local router communicates, and from which it requires authentication. The other router must have a hostname entry for the local router. This entry must have the same password as the local router has for this router. This command is useful for defining host names for special privileges. For example, a hostname `all` requiring no password could be created allowing the users to connect to general information without password.

Setting a hostname using this command takes precedence over setting a hostname in the kernel. If you set the hostname using the CLI, and then set the hostname in the kernel, the hostname set using the CLI will remain.

2.21.4 Examples

The following example sets the hostname to IPI, and shows the change in the prompt:

```
# configure terminal
(config)# hostname IPI
IPI(config)#
```

2.21.5 Validation Commands

`show running-config`

For sample output of the validation commands, refer Appendix A, *hostname on page 243*.

2.22 interface

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

2.22.1 Command Syntax

`interface IFNAME`

`IFNAME` = Specifies the name of the interface

2.22.2 Command Mode

Configure mode

2.22.3 Examples

This example shows the use of this command to enter the `Interface` mode (note the change in the prompt).

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

2.23 ip-access-group

Use this command to set up an IP access group for filtering either inbound or outbound packets on a particular interface. Use the `no` with this command to remove the IP access group.

2.23.1 Command Syntax

`ip-access-group (<1-199>|<1300-2699>|WORD) (in|out)`

`<1-199>` = IP access list (standard or extended)

`<1300-2699>` = IP expanded access list (standard or extended)

`WORD` = IP ZebOS acess-list name

`in` = To filter inbound packets

`out` = To filter outbound packets

`no ip-access-group (<1-199>|<1300-2699>|WORD) (in|out)`

2.23.2 Command Mode

Interface mode

2.23.3 Usage

This command is used for configuring an access group on an interface.

2.23.4 Example

```
(config-if)# ip-access-group 99 in
```

2.24 ip prefix-list

Use this command to create an entry for a prefix list. Use the no parameter with this command to delete the prefix-list entry.

This command is available only if LAYER3SRS is licensed.

2.24.1 Command Syntax

```
(no) ip prefix-list sequence number
(no) ip prefix-list LISTNAME description (.LINE)
(no) ip prefix-list LISTNAME|SEQ
```

LINE = Text description of the prefix list

LISTNAME = Specifies the name of a prefix list

SEQ = seq <

1-429496725> = (deny|permit) IPPREFIX any|LENGTH

seq <1-429496725> = The sequence number of the prefix list

deny = Specifies that packets are to be rejected

permit = Specifies that packets are to be accepted

IPPREFIX=A.B.C.D/M = The IP address mask and length of the prefix list mask

any = Takes all packets of any length. This parameter is the same as using `0.0.0.0/0 le 32` for `IPPREFIX`.

`LENGTH= [LE|GE]`

`LE= le <0-32>` Maximum prefix length to be matched

`GE= ge <0-32> =` Minimum prefix length to be matched.

2.24.2 Command Mode

Configure mode

2.24.3 Usage

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `GE` and `LE` specify the range of the prefix length to be matched. When setting these parameters, set the `LE` value to be less than 32, and the `GE` value to be less than `LE` value.

In this configuration, the `ip prefix-list` command matches all, but denies the IP address range, 76.2.2.0.

```
router bgp 100
network 172.1.1.0
network 172.1.2.0
neighbor 10.6.5.3 remote-as 300
neighbor 10.6.5.3 prefix-list mylist out
!
!
ip prefix-list mylist seq 5 deny  76.2.2.0/24
ip prefix -list mylist seq 10 permit 0.0.0.0/0
```

2.24.4 Examples

```
# configure terminal
(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8 le 22 ge 14
```

2.24.5 Related Commands

`match ip address, neighbor prefix-list, match route-map`

2.25 ipv6 access-list

Use this command to configure an access list for filtering frames. Use the `no` parameter to remove a specified access-list.

This command is available only if LAYER3SRS is licensed.

2.25.1 Command Syntax

`(no) ipv6 access-list LISTNAME (DENY|PERMIT|REMARK)`

`LISTNAME = WORD DENY|PERMIT|REMARK =` IP SRstackware access-list

`DENY = deny [X:X::X:X/M (exact-match)]|any =` Specify route to reject

`PERMIT = permit [X:X::X:X/M (exact-match)]|any =` Specify route to permit

`A.B.C.D =` An IPv6 address.

`M =` Mask Specifying which part of the IPv6 address will be ignored

`any =` Allows any IPv6 address or prefix to match

`exact-match =` Specifies exact-matching of prefixes

`REMARK = remark .LINE`

`LINE =` Multi-line, access-list entry comment up to 100 characters

2.25.2 Command Mode

Configure mode

2.25.3 Usage

Use access lists to control the transmission of packets on an interface, and restrict contents of routing updates. The switch stops checking the access list after a match occurs.

2.25.4 Examples

```
# configure terminal
(config)# ipv6 access-list mylist deny 3ffe:506::/32 exact-match
(config)# ipv6 access-list mylist permit any
```

2.25.5 Validation Commands

`show running-config, show ipv6 access-list`

For sample output of the validation commands, refer Appendix A, *ipv6 access-list on page 244*.

2.26 ipv6 prefix-list

Use this command to create an entry for an ipv6 prefix-list.

This command is available only if LAYER3SRS is licensed.

2.26.1 Command Syntax

```
(no) ipv6 prefix-list sequence number
     ipv6 prefix-list description .LINE
(no) ipv6 prefix-list description (.LINE)
(no) ipv6 prefix-list LISTNAME|SEQ
```

`LINE` = Text description of the prefix list

`LISTNAME` = Specifies the name of a prefix list

`SEQ = seq <1-429496725> (deny|permit) IPPREFIX any|LENGTH`

`seq <1-429496725>` = The sequence number of the prefix list

`deny` = Specifies that packets are to be rejected

`permit` = Specifies that packets are to be accepted

`IPPREFIX = X:X::X:X/M` = The IP address mask and length of the prefix list mask

`any` = Takes all packets of any length. This parameter is the same as using `0.0.0.0/0 le 32` for `IPPREFIX`.

`LENGTH= [LE|GE]`

`LE= le <0-32>` Maximum prefix length to be matched

`GE= ge <0-32>` Minimum prefix length to be matched

2.26.2 Command Mode

Configure mode

2.26.3 Usage

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `GE` and `LE` specify the range of the prefix length to be matched.

2.26.4 Examples

```
ipv6 prefix-list mylist seq 12345 deny 3ffe:345::/16 le 22 ge 14
```

2.27 line vty

Use the `line vty` command to move or change to VTY mode.

2.27.1 Command Syntax

`line vty [FIRST] (LAST)`

`FIRST <0-871> =` Specify the first line number

`LAST <0-871> =` Specify the last line number

2.27.2 Command Mode

Configure mode

2.27.3 Usage

This command is used to telnet to the NSM or any protocol daemons. This configuration is necessary for any telnet session. This configuration should be in the daemon's config file before starting the daemon.

Use this command to enter the line mode to configure the `access-class`, and set the `exec-timeout`.

2.27.4 Examples

The following example shows the use of the `line` command to enter the Line command mode (note the change in the prompt).

```
# configure terminal
(config)# line vty 3
(config-line)#
```

2.27.5 Validation Commands

`show running-config`

For sample output of the validation commands, refer Appendix A, *line vty on page 246*.

2.28 log file

Use the `log file` command to specify log file controls, and where to save the logs in a configuration file. Use the `no` parameter to revert logging to the default file.

2.28.1 Command Syntax

```
   log file FILENAME
no log file (FILENAME)
```

`FILENAME` = Specifies the file name of the log

2.28.2 Command Mode

Configure mode

2.28.3 Usage

The log file is written to `filename` in the default location, usually `usr/local/sbin`.

2.28.4 Examples

This command is used to log the debug messages of a particular protocol daemon to the specified file.

```
Router# configure terminal
Router(config)# log file /usr/local/sbin/bgpd.log
```

2.28.5 Validation Commands

```
show running-config
```

For sample output of the validation commands, refer to *Appendix A, log file on page 247*.

2.29 log record-priority

Use the `log record-priority` command to include the priority of the message within the entry in the log file. Use the `no` parameter to exclude the priority from the entry.

2.29.1 Command Syntax

```
(no) log record-priority
```

2.29.2 Command Mode

Configure mode

2.29.3 Examples

```
# configure terminal
(config)# log record-priority
```

2.29.4 Validation Commands

```
show running-config
```

For sample output of the validation commands, refer Appendix A, *log record-priority on page 249*.

2.30 log syslog

Use the `log syslog` command to begin the logging of information to system log and set the level to debug. Use the `trap` parameter and its subparameters to set the logging to a different level. Use the `no` parameter to disable logging to the system log.

2.30.1 Command Syntax

```
  log syslog
no log syslog
```

2.30.2 Command Mode

Configure mode

2.30.3 Usage

The syslog enables logging and analyzing configuration events and system error messages, centrally. This helps in monitoring interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug output sessions.

2.30.4 Examples

```
# configure terminal
(config)# log syslog
```

2.30.5 Validation Commands

None.

2.31 log trap

Use the `log trap` command with the log file to specify system message logging levels. Use the `no` parameter to include all levels of logging.

2.31.1 Command Syntax

```
   log trap PRIORITY
no log trap
PRIORITY = emergencies|alerts|critical|errors|warnings|
       notifications|informational|debugging
```

`emergencies` = Turns on logging of only the most severe messages

`alerts` = Turns on logging of the above plus this level

`critical` = Turns on logging of the above plus this level

`errors` = Turns on logging of the above plus this level

`warnings` = Turns on logging of the above plus this level

`notifications` = Turns on logging of the above plus this level

`informational` = Turns on logging of the above plus this level

`debugging` = Turns on logging of the above plus this level. This level of logging is the most comprehensive.

2.31.2 Command Mode

Configure mode

2.31.3 Examples

```
# configure terminal
(config)# log trap alerts
(config)# log trap critical
(config)# log trap informational
```

2.31.4 Validation Commands

`show running-config`

For sample output of the validation commands, refer Appendix A, *log trap on page 252*.

2.31.5 Related Commands

`log file`

2.32 login

Use this command to set a password prompt before entering the configuration mode, and enable password checking.

2.32.1 Command Syntax

`(no) login`

2.32.2 Default

Enabled

2.32.3 Command Mode

Line mode

2.32.4 Usage

Login is enabled by default. The `no login` command allows users to connect directly to the Privileged Exec mode skipping the password verification prompt. After using the `no login` command, if the user changes to the `login` command again, the system uses the password used earlier, unless the user specifies a password in the configure mode (see the following example).

2.32.5 Example

The following examples show the use of `login` and `no login` command. In this example, a password `pass` is set (in configure mode) before using the `login` command.

```
!
# configure terminal
(config)# line vty 3
(config-line)# no login
!
!
# configure terminal
#(config)# password pass
#(config)# line vty
#(config-line)# login
!
```

2.33 mac-learning

Use this command to enable/disable the MAC learning. MAC learning configuration is per port level.

2.33.1 Command Syntax

`mac-learning (enable|disable)`

By default it is enable.

2.33.2 Command Mode

Interface mode

2.33.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# mac-learning disable
```

2.33.4 Validation Commands

`show running-config interface`

NOTICE

Configuration of **`no bridge-acquire`** will take higher priority over **`mac-learning enable`** configuration on reboot.

2.34 match as-path

Use this command to match an autonomous system path access list. Use the no parameter with this command to remove a path list entry.

This command is available only if LAYER3SRS is licensed.

2.34.1 Command Syntax

```
   match as-path LISTNAME
no match as-path
no match as-path LISTNAME
```

`LISTNAME` - Specifies as autonomous system path access list name

2.34.2 Command Mode

Route-map mode

2.34.3 Usage

The `match as-path` command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are `not` met then the route is neither accepted nor forwarded, irrespective of `permit` or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid only for BGP.

2.34.4 Examples

```
# configure terminal
(config)# route-map myroute deny 34
(config-route-map)# match as-path myaccesslist
```

2.34.5 Related Commands

`match metric, match ip address, match community, set as-path, set community`

2.35 mac-ageing-time

Use this command to specify the ageing-out time for a learned MAC address on a unit. The learned MAC address persists until the specified time.

2.35.1 Command Syntax

`mac-ageing-time <unit> <AGEINGTIME>`

`no mac-ageing-time (base|fabric)`

`unit = base|fabric`

`AGEINGTIME = <10-1000000> = The number of seconds of persistence`

2.35.2 Command Mode

Configure mode

2.35.3 Default

The default ageing time is 300 seconds.

2.35.4 Examples

```
# configure terminal
(config)# mac-ageing-time base 500
```

2.36 match community

Use this command to specify the community to be matched. Use the no parameter with this command to remove the community list entry.

This command is available only if LAYER3SRS is licensed.

2.36.1 Command Syntax

`match community WORD`

`no match community`

```
no match community WORD
```

`WORD` = Specifies the Community-list name

2.36.2 Command Mode

Route-map mode

2.36.3 Usage

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

Use the `match community` command to allow matching based on community lists.

The values set by the `match community` command overrides the global values. The route that does not match at least one match clause is ignored.

This command is valid only for BGP.

2.36.4 Examples

```
# configure terminal
(config)# route-map myroute permit 3
(config-route-map)# match community mylist
```

2.36.5 Related Commands

`match ip address, match as-path, set as-path, set community, match metric`

2.37 match interface

Use this command to define the interface match criterion. Use the `no` parameter with this command to remove the specified match criterion.

This command is available only if LAYER3SRS is licensed.

2.37.1 Command Syntax

```
match interface IFNAME
no match interface
```

`IFNAME` = A string that specifies the interface for matching

2.37.2 Default

Disabled

2.37.3 Command Mode

Route-map mode

2.37.4 Usage

The `match interface` command specifies the next-hop interface name of a route to be matched.

This command is only valid for RIP, OSPF, and IS-IS.

2.37.5 Example

```
# configure terminal
(config)# route-map mymap1 permit 10
(config-route-map)# match interface eth0
```

2.37.6 Related Commands

`match tag, match route-type external`

2.38 mirror interface

Use this command to define a mirror source port and its direction. This command must be run separately for each source port.

Use the `no` parameter with this command to disable port mirroring by the destination port on the specified source port.

NOTICE

For base chipset: You can configure in total, "2 transmit MTPs and 4 receive MTPs" or "2 transmit and receive both MTPs and 2 receive MTPs".

For Fabric chipset : You can configure in total , "4 egress MTPs" or "2 egress and ingress both MTPs" or "4 ingress MTPs".

Where MTP is alias for mirror-to-port or destination port.

Each packet can be mirrored up to 2 copies.

NOTICE

L2 port can be mirrored only on L2 port.

L3 port can be mirrored only on L3 port.

2.38.1 Command Syntax

`mirror interface SOURCEPORT direction SNOOPDIRECTION`

`no mirror interface SOURCEPORT`

`SOURCEPORT` = Name of the Source interface to be used

`SNOOPDIRECTION [both|receive|transmit]`

`both` = Specifies mirroring of traffic in both directions

`receive` = Specifies mirroring of received traffic

`transmit` = Specifies mirroring of transmitted traffic

2.38.2 Command Mode

Interface mode

2.38.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# mirror interface eth1 direction both
```

2.39 match ip address

Use this command to specify the match address of route. Use the `no` parameter with this command to remove the `match ip address` entry.

This command is available only if LAYER3SRS is licensed.

2.39.1 Command Syntax

```
   match ip address ACCESSLISTID
no match ip address
no match ip address ACCESSLISTID
ACCESSLISTID = WORD|<1-199>|<1300-2699>
```

`WORD` = The name of IP access-list

`<1-199>` = The IP access-list number

`<1300-2699>` = The IP access-list number (expanded range)

2.39.2 Command Mode

Route-map mode

2.39.3 Usage

The `match ip address` command specifies the IP address to be matched. If there is a match for the specified IP address, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified then the route is not redistributed or controlled. If the match criteria are `not` met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid for BGP, OSPF, RIP, and IS-IS only.

2.39.4 Examples

```
# configure terminal
(config)# route-map myroute permit 3
(config-route-map)# match ip address List1
```

2.39.5 Related Commands

`match community, match as-path, set as-path, set community, match metric`

2.40 match ip address prefix-list

Use this command to match entries of prefix-lists. Use the `no` parameter with this command too disable this function

This command is available only if LAYER3SRS is licensed.

2.40.1 Command Syntax

```
match ip address prefix-list LISTNAME
```

```
no match ip address prefix-list LISTNAME
```

`LISTNAME` = Specifies the IP prefix list name

2.40.2 Command Mode

Route-map mode

2.40.3 Usage

This command specifies the entries of prefix-lists to be matched. If there is a match for the specified prefix-list entries, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables..

This command is valid for BGP, OSPF, and RIP only.

2.40.4 Examples

```
# configure terminal
(config)# route-map rmap1 permit 3
(config-route-map)#match ip address prefix-list mylist
```

2.41 match ip next-hop

Use this command to specify a next-hop address to be matched in a route-map. Use the `no` parameter with this command to disable this function.

This command is available only if LAYER3SRS is licensed.

2.41.1 Command Syntax

`match ip next-hop ACCESSLISTID`

`no match ip next-hop`

`no match ip next-hop ACCESSLISTID`

`ACCESSLISTID = WORD|<1-199>|<1300-2699>|PREFIXLIST =` Specifies the IP access list name

`WORD =` The IP access-list name

`<1-199> =` The IP access-list number

`<1300-2699> =` The IP access-list number (expanded range)

`PREFIXLIST prefix-list WORD =` Match entries of prefix-lists

`WORD =` IP prefix-list name

2.41.2 Command Mode

Route-map mode

2.41.3 Usage

The `match ip next-hop` command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and `permit` is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid for BGP, OSPF, RIP, and IS-IS only.

2.41.4 Examples

```
# configure terminal
```

```
(config)# route-map rmap1 permit 3
(config-route-map)# match ip next-hop mylist
```

2.41.5 Related Commands

`match community, match as-path, set as-path, set community, match metric`

2.42 match ip next-hop prefix-list

Use this command to specify the next-hop IP address match criterion, using the prefix-list. Use the no parameter with this command to remove the specified match criterion.

This command is available only if LAYER3SRS is licensed.

2.42.1 Command Syntax

```
(no) match ip next-hop prefix-list LISTNAME
 no match ip next-hop prefix-list
```

`LISTNAME` = A string specifying the prefix-list name

2.42.2 Default

Disabled

2.42.3 Command Mode

Route-map mode

2.42.4 Usage

Use the `match ip next-hop` prefix-list command to match the next-hop IP address of a route.

This command is valid for BGP and RIP only.

2.42.5 Examples

```
# configure terminal
(config)# route-map mymap permit 3
(config-route-map)# match ip next-hop prefix-list list1
```

2.42.6 Related Commands

`match metric, match interface, match ip next-hop`

2.43 match ipv6 address

Use this command to specify the match address of route. Use the `no` parameter with this command to remove the `match ip address` entry.

This command is available only if LAYER3SRS is licensed.

2.43.1 Command Syntax

```
match ipv6 address WORD
```

```
no match ipv6 address WORD
```

`WORD` = Specifies the IPv6 access list name

2.43.2 Command Mode

Route-map mode

2.43.3 Usage

The `match ipv6 address` command specifies the IPv6 address to be matched. If there is a match for the specified IPv6 address, and `permit` is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid for BGP, RIPng, and IS-IS only.

2.43.4 Examples

```
# configure terminal
(config)# route-map ipi deny 1
(config-route-map)# match ipv6 address ipi
```

2.44 match ipv6 address prefix-list

Use this command to match entries of prefix-lists. Use the no parameter with this command to disable this function.

This command is available only if LAYER3SRS is licensed.

2.44.1 Command Syntax

```
   match ipv6 address prefix-list LISTNAME
no match ipv6 address prefix-list LISTNAME
```

`LISTNAME` = Specifies the IPv6 prefix list name

2.44.2 Command Mode

Route-map mode

2.44.3 Usage

The `match ipv6 address prefix-list` command specifies the entries of prefix-lists to be matched. If there is a match for the specified prefix-list entries, and `permit` is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables. .

This command is valid for BGP, OSPFv3, and RIPng only.

2.44.4 Examples

```
# configure terminal
(config)# route-map rmap1 permit 3
(config-route-map)#match ipv6 address prefix-list mylist
```

2.45 match ipv6 next-hop

Use this command to specify a next-hop address to be matched by the route-map. Use the no parameter with this command to disable this function.

This command is available only if LAYER3SRS is licensed.

2.45.1 Command Syntax

```
   match ipv6 next-hop X:X::X:X|WORD
no match ipv6 next-hop X:X::X:X|WORD
```

`X:X::X:X` = The IPv6 address

`WORD` = The IPv6 access-list name

2.45.2 Command Mode

Route-map mode

2.45.3 Usage

The `match ipv6 next-hop` command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and `permit` is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid for BGP and IS-IS only.

2.45.4 Examples

```
# configure terminal
(config)# route-map rmap1 permit 3
(config-route-map)# match ipv6 next-hop 3ffe::1
```

2.46 match metric

Use this command to match a metric of a route. Use the `no` parameter with this command to disable this function.

This command is available only if LAYER3SRS is licensed.

2.46.1 Command Syntax

`match metric METRIC`

`no match metric METRIC`

`METRIC <0-4261412864>` = Specifies the metric value

2.46.2 Command Mode

Route-map mode

2.46.3 Usage

The `match metric` command specifies the metric to be matched. If there is a match for the specified metric, and `permit` is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid for BGP, OSPF, RIP, and IS-IS only.

2.46.4 Examples

```
# configure terminal
(config)# route-map myroute permit 3
(config-route-map)# no match metric 888999
```

2.46.5 Related Commands

`match community`, `match as-path`, `set as-path`, `set community`, `match ip next-hop`

2.47 match origin

Use this command to match origin code. Use the no parameter with this command to disable this matching.

This command is available only if LAYER3SRS is licensed.

2.47.1 Command Syntax

`(no) match origin (egp|igp|incomplete)`

`egp` = Learned from EGP

`igp` = Local IGP

`incomplete` = Unknown heritage

2.47.2 Command Mode

Route-map mode

2.47.3 Usage

The origin attribute defines the origin of the path information. The `egp` parameter is indicated as an `e` in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The `igp` parameter is indicated as an `i` in the routing table, and it indicates the origin of the path information is interior to the originating AS. The `incomplete` parameter is indicated as a `?` in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

The `match origin` command specifies the origin to be matched. If there is a match for the specified origin, and `permit` is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

This command is valid for BGP only.

2.47.4 Example

```
# configure terminal
(config)#  route-map myroute deny 34
(config-route-map)#  match origin egp
```

2.47.5 Related Commands

None.

2.48 match route-type

Use this command to match specified external route type. Use the no parameter with this command to turn off the matching.

This command is available only if LAYER3SRS is licensed.

2.48.1 Command Syntax

```
(no) match route-type external (type-1 | type-2)
```

2.48.2 Default

Disabled

2.48.3 Command Mode

Route-map mode

2.48.4 Usage

Use the match `route-type external` command to match specific external route types. AS-external LSA is either Type-1 or Type-2. `External type-1` matches only Type 1 external routes, and `external type-2` matches only Type 2 external routes.

This command is valid for OSPF only.

2.48.5 Examples

```
# configure terminal
(config)# route-map mymap1 permit 10
(config-route-map)# match route-type external type-1
```

2.48.6 Related Commands

`match tag, match route-type external`

2.49 match tag

Use this command to match the specified tag value. Use the `no` parameter with this command to turn off the declaration.

This command is available only if LAYER3SRS is licensed.

2.49.1 Command Syntax

`(no) match tag <0-4294967295>`

2.49.2 Default

Disabled

2.49.3 Command Mode

Route-map mode

2.49.4 Usage

Use the `match tag` command to match the specified tag value.

This command is valid for OSPF only.

2.49.5 Examples

```
# configure terminal
(config)# route-map mymap1 permit 10
(config-route-map)# match tag 100
```

2.49.6 Related Commands

`match metric, match route-type external`

2.50 maximum-paths

Use this command to enable multipath support on SRstackware, and set the maximum number of paths to be installed in the FIB (Forward Information Base). Use the `no` parameter with this command to revert to default.

Currently, this command is available on Linux systems only.

2.50.1 Command Syntax

`(no) maximum-paths <1-10>`

```
no maximum-paths
```

<1-10> = Specify the maximum number of paths to be installed in the FIB

2.50.2 Default

By default, the maximum number of paths is set to 4.

2.50.3 Command Mode

Configure mode

2.50.4 Example

```
# configure terminal
(config)# maximum-paths 5
```

2.51 mtu

Use this command to set the Maximum Transmission Unit (MTU) size of an interface. This command must not be used on aggregator interfaces.

2.51.1 Command Syntax

```
mtu SIZE
```

SIZE = <68-9216> Specifies the size of MTU in bytes

2.51.2 Command Mode

Interface mode

2.51.3 Example

```
# configure terminal
(config)# interface eth0
(config-if)# mtu 120
```

2.51.4 Validation Commands

show interface

2.52 multicast

Use this command to set the multicast flag to an interface. Use the no form of this command to disable this function.

2.52.1 Command Syntax

```
(no) multicast
```

2.52.2 Command Mode

Interface mode

2.52.3 Examples

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

2.52.4 Validation Commands

```
show running-config
```

2.53 route-map

Use this command to enter the route-map mode, and to permit or deny match/set operations.

This command is available only if LAYER3SRS is licensed.

2.53.1 Command Syntax

`(no) route-map MAPTAG deny|permit SEQ`

`MAPTAG` = Identifies the route

`deny` = Route map denies set operations

`permit` = Route map permits set operations

`SEQ= <1-65535>` = Specifies the sequence number for insertion or deletion

2.53.2 Command Mode

Configure mode

2.53.3 Usage

Route-map is used to control and modify routing information. The route-map command allows redistribution of routes. It has a list of `match` and `set` commands associated with it. The match commands specify the conditions under which redistribution is allowed, and the `set` commands specify the particular redistribution actions to be performed if the criteria enforced by match commands are met. Route maps are used for detailed control over route distribution between routing processes.

Route maps also allow policy routing, and might route packets to a different route than the obvious shortest path.

If the `permit` parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the `match` criteria are not met, the next route map with the same tag is tested.

If the `deny` parameter is specified, and the match criteria are met, the route is not redistributed, and any other route maps with the same map tag are not examined.

Specify the `sequence` parameter to indicate the position a new route map is to have in the list of route maps already configured with the same name.

If you do not specify any match conditions in a route-map, then that route-map matches all routes.

2.53.4 Examples

The following example shows the use of the `route-map` command to enter the `route-map` mode (note the change in the prompt), and the use of this mode in match and set commands.

```
# configure terminal
(config)# route-map route1 permit 1
(config-route-map)# match as-path 60
(config-route-map)# set weight 70
```

2.54 paired-link

Use this command to configure a L2 link as backup for a specified active L2 link. These links are called paired-links. Failover mode can optionally be specified as preemptive or non-preemptive. The default mode is non-preemptive. You can use the no `paired-link` command to delete the paired-link.

2.54.1 Command Syntax

`(no) paired-link <active port> <backup port> (preemptive (DELAY) | nonpreemptive)`

`active port` = Any L2 link of the switch including ge/xe/po/sa

`backup port` = Any L2 link of the switch including ge/xe/po/sa

`DELAY` = Is the preemption delay till which the backup link continues in active role before the active link assumes the active role. The range is 1-60sec. Default value is 30sec.

2.54.2 Command Mode

Configure mode

2.54.3 Usage

This command is used to configure a L2 link as backup to a specified active L2 link. A link can be either a single port/interface or a combination of multiple interfaces/ports operating in link aggregation (static or with LACP). A port can act as backup for only one port of its own type. That is, a po port can act as backup for one po port alone and it cannot act as a backup for sa port.

A port can be part of only one paired-link. Neither active port or backup port can be part of etherchannel/portchannel. But two etherchannels/portchannels can be configured as paired-links.

Paired-links cannot be configured on the links, if Spanning Tree protocols are enabled on that link.

A link is said to be standby, if it assumes non-active role. Only active links will be forwarding and receiving packets. Standby links do not forward packets and it drop packets on receive.

A link failover is initiated, if the active link is down. An active link is considered as down, if the link status of at least one interface member is down. This could be caused from accidental cable removal or reboot of peer node or if an active link is down due to execution of shutdown command or port damage.

On failover, all MAC addresses learned on the previous active link are deleted. In case of a link failure between a payload and a controller, the failover feature leads to an isolation of the payload for traffic inside the ATCA system. This is because the payload would switch to the standby network plane, but all other node blades inside the ATCA system stay with their active network plane.

Two types of failover modes are configurable:

- Preemptive - If the active link goes operationally down, the standby takes over and assumes active role. If the former active link comes operationally up again, the system automatically restores to the original setup. The standby link only forwards traffic in case the active link is down.
- Non-preemptive mode - If the active link goes operationally down, the standby takes over and assumes active role. If the former active link comes operationally up again, the system remains in the current state. The former active link assumes the standby role. This is the default mode.

If you change the failover mode from non-preemptive to preemptive, where the configured active link is UP and running but is current standby, then the preemptive timer starts and on expiry of this timer, configured active takes over the role as current active.

2.54.4 Examples

```
# configure terminal
(config)# paired-link ge1 ge3 preemptive 40
(config)# paired-link sa1 sa2
(config)# no paired-link ge1 ge3
```

2.55 service advanced-vty

Use this command to set multiple options to be listed when the Tab key is pressed, after completing a command. Use the no parameter to set no options to be listed when the Tab key is pressed, after completing a command.

2.55.1 Command Syntax

`(no) service advanced-vty`

`advanced-vty` = Enable advanced mode VTY interface

2.55.2 Command Mode

Configure mode

2.55.3 Usage

This feature applies to commands with more than one option.

2.55.4 Examples

```
# configure terminal
(config)# service advanced-vty
```

2.56 service password-encryption

Use this command to specify encryption of passwords. Use the no parameter to disable this feature.

When using the `service password-encryption` command through IMISH, you must write to memory using the `write memory` or `write file` command. If you have not written to memory, the change made by this command (encryption) is not available when you log into IMISH the next time.

2.56.1 Command Syntax

`(no) service password-encryption`

`password-encryption` = Enable encrypted passwords

2.56.2 Command Mode

Configure mode

2.56.3 Usage

The `service password-encryption` command specifies encryption of the passwords. This encryption is simple, and designed to prevent casual observers from reading passwords not for serious hackers. The following output displays the encrypted password.

```
Router# configure terminal
Router(config)# service password-encryption
Current configuration:
!
hostname SRstackware
password 8 aZSABJxOet0gs
enable password 8 SLtKyTiWDXTZw
!
```

2.56.4 Examples

```
# configure terminal
(config)# service password-encryption
```

2.56.5 Validation Commands

`enable password`

2.57 service terminal-length

Use this command to set the terminal length for VTY sessions. Use the `no` parameter to disable this feature.

2.57.1 Command Syntax

`(no) service terminal-length LINES`

`terminal-length` = Establish system-wide terminal length configuration

`LINES = <0-512>` = Number of lines of VTY (0 means no line control)

2.57.2 Command Mode

Configure mode

2.57.3 Usage

The `terminal-length` parameter sets the terminal length for VTY sessions. In the following configuration, the terminal length for VTY sessions will be set to 60, making 60 the number of terminal lines for any telnet session.

```
# configure terminal
(config)# service terminal-length 60
```

2.57.4 Examples

```
# configure terminal
(config)# service advanced-vty
```

2.57.5 Validation Commands

`show running-config`

2.58 set aggregator

Use this command to set the AS number for the route map and router ID. Use the `no` parameter with this command to disable this function

2.58.1 Command Syntax

`(no) set aggregator as ASNUM IPADDRESS`

`ASNUM` = Specifies the AS number of aggregator. For 2 byte BGP speakers, the valid range for ASNUM is <1-65535>, and <1-4294967295> for 4 byte speakers.

`IPADDRESS` = Specifies the IP address of aggregator

2.58.2 Command Mode

Route-map mode

2.58.3 Usage

An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the `set aggregator` command to assign an AS number for the aggregator.

To use the `set aggregator` command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

This command is valid for BGP only.

2.58.4 Examples

```
# configure terminal
(config)# route-map myroute permit 3
(config-route-map)# set aggregator as 43 10.10.0.3
```

2.59 set as-path

Use this command to modify an autonomous system path for a route. Use the `no` parameter with this command to disable this function.

This command is available only if LAYER3SRS is licensed.

2.59.1 Command Syntax

`(no) set as-path prepend (.ASN)`

`prepend` = Prepends the autonomous system path

`ASN SRstackware` = Prepends this number to the AS path.

2.59.2 Command Mode

Router-map mode

2.59.3 Usage

Use the `set as-path` command to specify an autonomous system path. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use the `prepend` parameter with this command to prepend an AS path string to routes increasing the AS path length.

To use the `set as-path` command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

This command is valid for BGP only.

2.59.4 Examples

```
# configure terminal
(config)# route-map myroute permit 3
(config-route-map)# set as-path prepend 8 24
```

2.60 set ip next-hop

Use this command to set the specified next-hop value. Use the `no` parameter with this command to turn off the setting.

This command is available only if LAYER3SRS is licensed.

2.60.1 Command Syntax

`(no) set ip next-hop A.B.C.D`

`no set ip next-hop`

`A.B.C.D =` Specifies the IP address of the next-hop

2.60.2 Default

Disabled

2.60.3 Command Mode

Route-map mode

2.60.4 Usage

Use this command to set the next-hop IP address to the routes.

This command is valid for BGP, OSPF, and RIP only.

2.60.5 Examples

```
# configure terminal
(config)# route-map mymap permit 3
(config-route-map)# set ip next-hop 10.10.0.67
```

2.60.6 Related Commands

`set metric`

2.61 set metric

Use this command to set a metric value for a route. Use the `no` parameter with this command to disable this function.

This command is available only if LAYER3SRS is licensed.

2.61.1 Command Syntax

`set metric METRICVAL`

`no set metric (0-4261412864)`

`METRICVAL = <+/-metric>|<0-4261412864>` = The metric value

2.61.2 Command Mode

Route-map mode

2.61.3 Usage

This command sets the metric value for a route, and influences external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the `bgp always-compare-med` command.

To use the `set metric` command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

This command is valid for BGP, OSPF, OSPFv3, RIP, RIPng, and IS-IS.

2.61.4 Examples

```
# configure terminal
(config)# route-map rmap1 permit 3
(config-route-map)# set metric 600
```

2.62 set metric-type

Use this command to set the metric type for the destination routing protocol. Use the no parameter with this command to return to the default.

This command is available only if LAYER3SRS is licensed.

2.62.1 Command Syntax

`(no) set metric-type type1|type2`

`type1` = Select to set OSPF external type 1 metric

`type2` = Select to set OSPF external type 2 metric

`(no) set metric-type internal|external`

`internal` = Select to set IS-IS internal metric type

`external` = Select to set IS-IS external metric type

2.62.2 Command Mode

Route-map mode

2.62.3 Usage

The `set metric-type 1|2|type1|type2` command sets the type to either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

The `set metric-type 1|2|type1|type2` command is valid for OSPF and OSPFv3 only. The `set metric-type internal|external` command is valid for IS-IS only.

2.62.4 Examples

In this example the metric type of the destination protocol is set to OSPF external Type 1.

```
# configure terminal
(config)# route-map rmap1 permit 3
(config-route-map)# set metric-type 1
```

2.62.5 Related Commands

`redistribute, default-information`

2.63 set tag

Use this command to set a specified tag value. Use the `no` parameter with this command to return to the default.

This command is available only if LAYER3SRS is licensed.

2.63.1 Command Syntax

`(no) set tag TAGVALUE`

`TAGVALUE = <0-4294967295> =` Tag value for destination routing protocol

2.63.2 Command Mode

Route-map mode

2.63.3 Usage

Tag in this command is the route tag which is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. Also, with using route-map, SRstackware can tag the LSAs with the appropriate tag value. Sometimes, the tag matches with using route-map, and sometimes, the value may be used by another application.

This command is valid for OSPF only.

2.63.4 Examples

In the following example the tag value of the destination routing protocol is set to 6:

```
# configure terminal
(config)# route-map rmap1 permit 3
(config-route-map)# set tag 6
```

2.63.5 Related Commands

`redistribute, default-information`

2.64 show access-list

Use this command to display a list of IP access lists.

This command is available only if LAYER3SRS is licensed.

2.64.1 Command Syntax

`show access-list`

2.64.2 Command Mode

Privileged Exec mode

2.64.3 Examples

```
# show access-list
```

2.65 show cli

Use this command to display the CLI tree of the current mode.

2.65.1 Command Syntax

```
show cli
```

2.65.2 Command Mode

All command modes

2.65.3 Usage

This is a section of the sample output of the `show cli` command executed at the `Interface` mode.

```
+-ospf
  +-A.B.C.D
    +-authentication [no ip ospf (A.B.C.D|) authentication]
    +-authentication-key [no ip ospf (A.B.C.D|) authentication-key]
    +-cost [no ip ospf (A.B.C.D|) cost]
    +-database-filter [no ip ospf (A.B.C.D|) database-filter]
    +-hello-interval [no ip ospf (A.B.C.D|) hello-interval]
    +-message-digest-key
```

2.65.4 Examples

```
# show cli
```

2.66 show flowcontrol

Use this command to display flow control information on PAUSE enabled ports.

2.66.1 Command Syntax

```
show flowcontrol
```

2.66.2 Command Mode

Exec mode

2.66.3 Example

```
# show flowcontrol
```

2.66.4 Usage

The following is a sample output of the `show flowcontrol` command displaying flow control information:

```
# show flowcontrol
Port Send FlowControl Receive FlowControl RxPause TxPause
admin oper admin oper
----- ------- -------- ------- -------- ------- -------
ge1   on      on       on      on       0       0
xe1   on      on       off     off      0       0
```

NOTICE
This command will not display flow control information for PAUSE disable ports

2.67 show flowcontrol interface

Use this command to display flow control information.

2.67.1 Command Syntax

```
show flowcontrol interface IFNAME
```

`IFNAME` = Specifies the name of the interface to be displayed

2.67.2 Command Mode

Exec mode

2.67.3 Example

```
# show flowcontrol interface ge2
```

2.67.4 Usage

The following is a sample output of the show flowcontrol interface command displaying flow control information:

```
# show flowcontrol interface ge1
Port    Send  FlowControl    Receive  FlowControl  RxPause TxPause
        admin    oper        admin    oper
-----   ------- --------    ------- --------     ------- -------
ge1     on      on          on      on           0       0
```

NOTICE

This command will not display flow control information for PAUSE disable ports.

2.68 show history

Use the `show history` command to list the commands entered in the current session. The history buffer is cleared automatically upon reboot.

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, SRstackware CLI Environment*.

2.68.1 Command Syntax

```
show history
```

2.68.2 Command Mode

Exec mode and Privileged Exec mode

2.68.3 Examples

```
show history
```

2.68.4 Usage

Two sample results from the `show history` command:

```
IMI-CLI#show history
   1 en
   2 show ru
   3 con t
   4 route-map er deny 3
   5 exit
   6 ex
   7 di
```

Though some modes do not have the show history command, commands entered in those modes are listed from the Privileged mode. All command line entries are listed, even erroneous commands.

```
# show history
  1 show ip protocols
  2 show ip protocols rip
  3 show history
  4 enable
  5 config terminal
  6 show his
  7 interface eth0
  8 show history
  9 router rip
  10 end
  11 list
  12 con t
  13 router rip
  14 shoe history
```

```
15 show history
16 end
```

2.69 show interface

Use this command to display interface configuration and status.

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, SRstackware CLI Environment*.

2.69.1 Command Syntax

`show interface IFNAME(s)`

`IFNAME(S) =` Specifies the names of the interfaces for which the status and configuration information is desired.

"-" is to specify the interface range

"," is to delimit the list of interfaces

2.69.2 Command Mode

Exec mode and Privileged Exec mode

2.69.3 Usage

When the QoS feature is enabled for the interface, this is what this command displays:

```
Router#show interface ge2
Interface ge2
  Hardware is Ethernet
  Current HW addr: 0273.ed9d.0004
  Physical:0273.ed9d.0004
  Description: BC2 - Slot 8
  index 5002 metric 1 mtu 1500 duplex-full arp ageing timeout 0
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 1g
  VRRP Master of :  VRRP is not configured on this interface.
```

```
    input packets 0547, bytes 0187570, dropped 0541, multicast packets 00
    output packets 0541, bytes 0187186, multicast packets 00 broadcast
packets 06
    statistics last updated on, Thu Nov  3 12:53:08 2011
    nanoseconds: 481854800
```

2.69.4 Examples

```
#show interface ge1,ge3,ge5-ge6,xe1-xe3
```

2.70 show ip access-list

Use this command to display a IP access lists.

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, SRstackware CLI Environment*.

This command is available only if LAYER3SRS is licensed.

2.70.1 Command Syntax

```
show ip access-list
```

2.70.2 Command Mode

Privileged Exec mode

2.70.3 Usage

The following is a sample output of the `show ip access-list` command showing the IP access-list entries.

```
# show ip access-list
Standard IP access list 1
    permit 172.168.6.0, wildcard bits 0.0.0.255
    permit 192.168.6.0, wildcard bits 0.0.0.255
```

2.70.4 Examples

```
#  show ip access-list
```

2.71 show ip prefix-list

Use this command to display the prefix list entries.

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, SRstackware CLI Environment*.

This command is valid for RIP and BGP protocols only.

This command is available only if LAYER3SRS is licensed.

2.71.1 Syntax Description

`show ip prefix-list (WORD|DETAIL|SUMMARY)`

`WORD=A.B.C.D/M (first-match|longer)`

`A.B.C.D` = IP address for the prefix list

`M=<0-32>` = The length of the address/Mask

`first-match` = The show command displays the first matching routing table for the given IP address or prefix

`longer` = Causes the show command to lookup longer prefix

`DETAIL` = Detail(WORD)

`WORD` = Name of prefix list

`SUMMARY`= Summary(WORD)

`WORD` = Name of prefix list

2.71.2 Command Mode

Exec mode

2.71.3 Usage

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
# show ip prefix-list
ip prefix-list ipi1: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```

2.71.4 Examples

```
# show ip prefix-list
# show ip prefix-list 10.10.0.98/8 first-match
# show ip prefix-list detail home
```

2.72 show list

Use this command to display a list of all the commands relevant to the current mode.

2.72.1 Command Syntax

`show list`

2.72.2 Command Mode

All command modes.

2.72.3 Usage

This is a section of the sample output of the `show list` command executed at the `Configure` mode.

```
(config)# show list
  access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
  access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
  access-list (<1-99>|<1300-1999>) (deny|permit) any
  access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D
  access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
  access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
```

2.72.4 Examples

```
# show list
```

2.73 show mirror

Use this command to display the status of all mirrored ports.

2.73.1 Command Syntax

```
show mirror
```

2.73.2 Command Mode

Privileged Exec mode

2.73.3 Example

```
# show mirror
```

2.73.4 Usage

The following is a sample output of the show mirror command displaying the status of all mirrored ports:

```
# show mirror
Mirror Test Port Name: ge1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: ge2
Mirror Test Port Name: ge3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: ge4
Mirror Test Port Name: ge3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: ge1
Mirror Test Port Name: ge1
```

```
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: ge3
Mirror Test Port Name: ge1
Mirror option: Enabled
Mirror direction: transmit
Monitored Port Name: ge4
```

2.74 show mirror interface

Use this command to display port mirroring.

2.74.1 Command Syntax

`show mirror interface IFNAME`

`IFNAME` = Specifies the name of the destination port

2.74.2 Command Mode

Interface, Privileged Exec and Exec mode

2.74.3 Example

```
# show mirror interface eth1
```

2.74.4 Usage

Following is a sample output of the `show mirror interface` command displaying mirroring information.

```
(config)# interface ge1
(config-if)# mirror interface ge2 direction both
(config-if)# show mirror interface ge2
Mirror Test Port Name: ge1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: ge2
```

2.75 show nsm client

Use this command to display NSM client information.

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 SRstackware Command Line Interface Environment chapter.

2.75.1 Command Syntax

```
show nsm client
```

2.75.2 Command Mode

Privileged Exec mode

2.75.3 Usage

This command displays the details of currently connected NSM clients, such as: the services requested by the protocols, statistics and the connection time. The following is a sample output for this command:

```
Router# show nsm client
NSM client ID: 1
  OSPF, socket 8
   Service: Interface Service, Route Service
   Message received 1, sent 6
   Connection time: Thu Sep 26 16:08:23 2002
```

2.75.4 Examples

```
# show nsm client
```

2.76 show route-map

Use this command to display user readable route-map information.

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, SRstackware CLI Environment on page 41*.

This command is available only if LAYER3SRS is licensed.

2.76.1 Command Syntax

`show route-map`

2.76.2 Command Mode

Privileged Exec mode

2.76.3 Usage

The following is a sample output of the `show route-map` command.

```
# show route-map
route-map ipi, permit, sequence 1
  Match clauses:
    metric 200
  Set clauses:
    metric 60
```

2.76.4 Examples

```
> show route-map
```

2.77 show running-config

Use the `show running-config` command to display the current configuration file.

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, SRstackware CLI Environment on page 41*.

2.77.1 Command Syntax

```
show running-config
```

2.77.2 Command Mode

Privileged Exec mode

2.77.3 Examples

```
show running-config
```

2.77.4 Usage

The display for the `show running-config` command is bracketed by `Current configuration` and `end`.

```
# show running-config

Current configuration:
!
hostname ripd
password zebra
log file /var/log/srstackware.log
!
debug rip events
debug rip packet
!
interface lo
!
interface cipcb0
!
```

```
interface sit0
!
interface eth0
!
interface eth1
 ip rip send version 2
 ip rip receive version 2
 ip rip authentication string !!!!
!
interface dummy0
!
interface ip6tnl0
!
interface ip6tnl1
!
!
router rip
 network eth0
 network eth1
 passive-interface eth0
 redistribute connected
!
ip prefix-list hoge seq 5 permit any
ip prefix-list hoge seq 10 permit 10.0.0.0/8
!
route-map nexthop permit 1
 set ip next-hop 10.10.0.97
!
line vty
 exec-timeout 0 0
!
end
```

2.77.5 Related Commands

```
write terminal
```

2.78 show paired-links

Use this command to display the configured paired-links.

2.78.1 Command Syntax

```
show paired-links
```

2.78.2 Command Mode

Exec mode

2.78.3 Examples

```
show paired-links
```

2.78.4 Usage

Sample output of show paired-links command is as follows:

```
Active Backup Current-Active   Mode   Delay   State
ge1    ge2    ge1       preempt 30 Active Up/Backup Up
xe3    xe4    xe4      preempt 1 Active Down/Backup Up
sa1    sa2     sa1    non-preempt NA Active Down(10g)/Backup Down (0g)
po1    po2    po2   non-preempt NA Active Up (20g)/Backup Up(20g)
ge5    ge6    ###   non-preempt NA Active Down(0g)/Backup Down(0g)
```

in Current-Active column means that none of the ports is assuming active role.

The delay in the command output always display the latest configured values.

2.79 show startup-config

Use the `show startup-config` command to display the startup configuration.

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, SRstackware CLI Environment on page 41*.

2.79.1 Command Syntax

```
show startup-config
```

2.79.2 Command Mode

Privileged Exec mode

2.79.3 Examples

```
show startup-config
```

2.79.4 Usage

The following is a sample output of the show startup-config command displaying the configuration at startup.

```
ripd# show startup-config
!
! SRstackware configuration saved from vty
!   2001/04/21 11:38:52
!
hostname ripd
password zebra
log file /var/log/srstackware.log
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
```

```
!
router rip
 redistribute connected
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line vty
 exec-timeout 0 0
```

2.80 show statistics

Use this command to display port (s) counters statistics.

NOTICE
Only non-zero interface statistics will be displayed.

2.80.1 Command Syntax

```
show statistics (interface IFNAME | )
```

2.80.2 Command mode

Exec mode and Privileged Exec mode

2.80.3 Usage

This shows the Tx/Rx counter’s statistics on the interface(s). The CLI displays non-zero objects among the below objects:

```
RX Statistics

rxPkts
rxOctets
rxUcastPkts
rxMulticastPkts
rxBroadcastPkts
rxOversizePkts
rxCtrlFrames
rxPauseFrames
```

```
rxMTUCheckError
rxUndersizeError
rxFragments
rxJabbers
rxSymbolErrors
rxCRCErrors
rxErrors
rxLengthErrors
rxPkts1519to1522Octets
rxCtrlUnknownOpcodes
rxPkts64Octets
rxStatsRxPkts65to127Octets
rxPkts128to255Octets
rxPkts256to511Octets
rxPkts512to1023Octets
rxPkts1024to1518Octets
rxPkts1519to2047Octets
rxPkts2048to4095Octets
rxPkts4096to9216Octets
rxAlignmentErrors
rxCarrierSenseErrors

TX Statistics

txPkts
txOctets
txUcastPkts
txMulticastPkts
txBroadcastPkts
txOversizePkts
txPauseFrames
txFragments
txCRCErrors
txPkts1519to1522Octets
txPkts64Octets
txPkts65to127Octets
txPkts128to255Octets
txPkts256to511Octets
txPkts512to1023Octets
txPkts1024to1518Octets
txPkts1519to2047Octets
```

```
txPkts2048to4095Octets
txPkts4096to9216Octets
txCtrlFrames
txJabber
txCollisions
txSingleCollisions
txMultipleCollisions
txExcessiveCollisions
txLateCollisions
txSingleDeferrals
txMultipleDeferrals
```

2.80.4 Examples

```
#show statistics interface ge45
#show statistic
```

2.81 show statistics interface IFNAME drop-counters

Use this command to display port's drop counter statistics.

2.81.1 Command Syntax

```
show statistics interface IFNAME drop-counters
```

2.81.2 Command Mode

Exec mode and Privileged Exec mode

2.81.3 Usage

This shows the Tx/Rx drop counter's statistics on the interface. The following is the sample output of this command.

```
#show statistics interface xe57 drop-counters
Interface xe57
RX Drop Statistics
  IfInDiscards                          : 00
  MCInDiscards                          : 00
```

```
  FP|PolicyDiscards                       : 00
  VLANInDiscards                          : 00
  FwdPbmpZeroDrop|Tunnel|ParityDiscards   : 00
  STPBlock|CellBufferPoolFullDiscards     : 00
  L3Discards                              : 00
  HG|DOS|LAG|MCErrorDiscards              : 00
TX Drop Statistics
  IfOutDiscards                           : 00
  MCOutDiscards                           : 00
  Ipv6IfStatsOutDiscards                  : 00
  STPBlockDiscards                        : 00
  L2MC|VXLTMissDiscards                   : 00
  VLANOutDiscards                         : 00
  AgedDiscards                            : 00
  HG|L2MTU|ParityDiscards                 : 00
  IPLen|SIP|LargeDiscards                 : 00
```

For more information on drop counters, see *Appendix B, Rx/Tx Drop Counters on page 263*.

2.81.4 Example

```
#show statistics interface xe57 drop-counters
```

2.82 show statistics vlan VLAN-ID

Use this command to display VLAN counter statistics.

NOTICE

VLAN statistics is supported only on Fabric chipset, but not on Base chipset.

2.82.1 Command Syntax

```
show statistics vlan VLAN-ID
```

2.82.2 Command Mode

Exec mode and Privileged Exec mode

2.82.3 Usage

This shows the Tx/Rx counter's statistics on the VLAN. The following is the sample output of this command.

```
#show statistics vlan 91
VLAN 91
RX Vlan Statistics
  InPkts                : 00          , InOctets                : 00
TX Vlan Statistics
  OutPkts               : 00          , OutOctets               : 00
```

2.82.4 Example

```
#show statistics vlan 91
```

2.83 show storm-control

Use this command to display storm control information for all interfaces, or for a particular interface.

2.83.1 Command Syntax

`show storm-control (IFNAME)`

`IFNAME` = Specifies the name of the interface for which storm-control information is to be displayed

2.83.2 Command Mode

Privileged Exec mode

2.83.3 Example

```
# show storm-control eth1
```

2.83.4 Usage

The following is a sample output of this command displaying storm control information:

```
# show storm-control eth1
Port BcastLevel McastLevel DlfLeve
fe14    40.0%     100.0%    100.0%
```

2.84 storm-control level

Use this command to specify the rising threshold level for broadcasting, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level. Use the `no` parameter with this command to disable storm control.

2.84.1 Command Syntax

`storm-control broadcast|multicast|dlf level LEVEL`

`no storm-control broadcast|multicast|dlf level`

`broadcast` = Broadcast lookup failure

`multicast` = Multicast lookup failure

`dlf` = Destination lookup failure

`LEVEL <0-100>` = Sets the percentage of the threshold; percentage of the maximum speed (pps) of the interface

2.84.2 Default

By default, storm control is disabled.

2.84.3 Command Mode

Interface mode

2.84.4 Usage

Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

The number of frames to be forwarded is calculated based on the fixed frame size of 1512 bytes. As a result, the number of frames dropped for a particular storm-control level does not vary with the frame size of the flooded traffic.

2.84.5 Example

```
(config)# interface eth0
(config-if)# storm-control broadcast level 30
```

2.85 show version

Use the `show version` command to display the version of SRstackware currently running.

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, SRstackware CLI Environment on page 41*.

2.85.1 Command Syntax

```
show version
```

2.85.2 Command Mode

Privileged Exec mode and Exec mode

2.85.3 Usage

The following is an output from the `show version` command.

```
SP5-B52#show version
ZebOS version 7.6.1 IPIRouter 04/07/14 18:41:33
 Build # is ZebOS-7-6-1-IPI on host i686-pc-linux-gnu
 Copyright (C) 2001-2004 IP Infusion Inc.  All rights reserved.
```

2.86 shutdown

Use this command to shut down the selected interface. Use the `no` form of this command to disable this function.

2.86.1 Command Syntax

`(no) shutdown`

2.86.2 Command Mode

Interface mode

2.86.3 Examples

The following example shows the use of the `shutdown` command to shut down the interface called `eth0`.

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

2.87 terminal length

Use the `terminal length` command to set number of lines displayed on a terminal. Use the `no` parameter with this command to revert to the default setting.

2.87.1 Command Syntax

`(no) terminal length LENGTH`

`LENGTH = <0-512> =` The number of lines on a terminal. The default length is 25 lines.

2.87.2 Command Mode

Exec mode and Privileged Exec mode

2.87.3 Examples

The following example sets the terminal length to 30 lines.

```
# terminal length 30
```

2.88 terminal monitor

Use the `terminal monitor` command to display debugging output on a terminal.

2.88.1 Command Syntax

`(no) terminal monitor`

2.88.2 Command Mode

Privileged Exec mode

2.88.3 Examples

```
# terminal monitor
```

2.88.4 Related Commands

All debug commands

2.89 who

Use the `who` command to display all other VTY connections.

This command is unavailable to SRstackware Server Routing Suite (SRS) customers and to SRstackware Advanced Routing Suite (ARS) customers using the IMISH for CLI management.

This command is only available on the Linux platform.

2.89.1 Command Syntax

`who`

2.89.2 Command Mode

Exec mode

2.89.3 Usage

The following is an output from the `who` command displaying all other VTY connections. The entry "*" marks the connection with the configuration rights.

```
Router# who
 vty[8] connected from 127.0.0.1.
*vty[9] connected from 127.0.0.1.
 vty[10] connected from 10.10.0.74
```

2.89.4 Examples

```
> who
```

2.90 write file and write memory

Use the `write file` or `write memory` command to write configuration data to a file.

2.90.1 Command Syntax

```
write file
write memory
```

2.90.2 Command Mode

Privileged Exec mode

2.90.3 Examples

```
# write file
```

2.90.4 Related Commands

`show running-config`

2.91 write terminal

Use the `write terminal` command to display current configurations to the VTY terminal.

2.91.1 Command Syntax

```
write terminal
```

2.91.2 Command Mode

Privileged Exec mode

2.91.3 Usage

The following is an output from the `write terminal` command displaying current configuration on the terminal.

```
ripd# write terminal

Current configuration:
!
hostname ripd
password zebra
log file /var/log/srstackware.log
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
```

```
 redistribute connected
!
line vty
 exec-timeout 0 0
!
end
```

2.91.4 Examples

```
# write terminal
```

2.91.5 Related Commands

show-running-config

Match-list Commands

3.1 match-list

Use the `match-list` command to configure a match list for performing various actions on the matched packets on the specified unit. Each Match-list ID is mapped to a group and thus allowing multiple matches to be made for a single incoming packet with one match per group. The following table lists the mapping:

Table 3-1 Match-list ID Mapping

Chip	Match-list IDs	Group	Number of Entries
Base	1-128	1	128
Base	129-256	2	128
Base	257-384	3	128
Base	385-512	4	128
Base	513-640	5	128
Base	641-768	6	128
Base	769-896	7	128
Base	897-1024	8	128
Fabric	1025-1152	9	128
Fabric	1153-1280	10	128
Fabric	1281-1536	11	256
Fabric	1537-1792	12	256
Fabric	1793-2048	13	256

This mapping results in eight groups on the base chip and five groups on the fabric chip, thus allowing a maximum of eight parallel matches for a packet received on the base chip and five parallel matches for a packet received on the fabric chip respectively.

Example: If the user wants a packet received on the fabric chip to be matched with two Match-list entries, then two entries must be created with Match-list ID 1025 and with Match-list ID 1153.

The support of IPv6-based qualifiers is optional. By default, the support will be disabled. The user needs to set the configuration parameter `ENABLE_IPV6_QUALIFIERS` to `YES` in `srsinit.conf` file to enable IPv6-based qualifiers and reboot the blade to make the configuration effect.

When the support for IPv6-qualifiers is enabled, 128 entries each in base and fabric will be reserved for IPv6 based Match-lists. The Match-list IDs that allow IPv6-based qualifiers are 1-128 in base and 1025-1152 in fabric. Also, note that since the IPv6-based qualifier-set requires a bigger group, 128 entries each in base and fabric become unusable. The following table lists the mapping:

Table 3-2 Match-list ID Mapping - IPv6-based Qualifiers

Chip	Match-list IDs	Group	Number of Entries
Base	1-128	1	128 [IPv6-Compatible]
Base	129-256	2	128 [Disabled/Unusable]
Base	257-384	3	128
Base	385-512	4	128
Base	513-640	5	128
Base	641-768	6	128
Base	769-896	7	128
Base	897-1024	8	128
Fabric	1025-1152	9	128 [IPv6-Compatible]
Fabric	1153-1280	10	128 [Disabled/Unusable]
Fabric	1281-1536	11	256
Fabric	1537-1792	12	256
Fabric	1793-2048	13	256

User-Defined Fields

User-Defined Fields (UDF) feature allows to create user-defined fields and match the packets based on them instead of pre-defined packet fields. UDF enables user to selectively configure which bytes of the packet need to be included as match criteria for the match-lists.

The UDF support is optional and by default, it is disabled.

To enable the UDF support:

1. Open the `srsinit.conf` file located at `/etc/opt/srstackware/config`.
2. Find the `ENABLE_UDF` parameter and set its value to "Yes".
   Set its value to "No" to disable UDF support.
3. Restart the blade to reflect the configuration settings.

Once the UDF support is enabled on the blade, 128 match-list entries in base and 256 match-list entries in fabric are reserved for matching only user-defined fields. These UDFs are used as qualifiers for the Match-list IDs 257-384 on the base chipset and 1281-1536 on the fabric chipset.

Range Checker

Range Checker feature allows to match a range of values in a specific field as part of a single match-list. This feature allows user to create a single match-list and specify the range of values to be matched and the corresponding action to be performed. In the absence of this feature, user may need to create multiple match-lists to match a range of values in a specific field.

NOTICE

Both Range Checker and UDF features cannot be enabled simultaneously on a device. By default, the Range Checker feature is enabled and it is disabled once UDF is enabled on the device.

3.1.1 Command Syntax

`match-list <match-list-id> <unit>`

`match-list-id =` integer of range 1-2048

`unit =` base|fabric

3.1.2 Command Mode

Configure mode

3.1.3 Usage

Use match-list to control the transmission of packets and to update various contents in the packets. This command takes you to Match-list mode, where you can specify various parameters to match the packets that flow through the specified unit.

3.1.4 Examples

```
# configure terminal
(config)# match-list 2 base
(config-mlist)#
```

3.1.5 Validation Commands

`show running-config, show rule match-list`

3.2 match-list-priority

A priority can be assigned to each individual match-list by making the higher prioritized match-list to be matched first among all the possible matches in the group.

3.2.1 Command Syntax

```
match-list-priority <match-list-id> <0-2147483647>
match-list-id = integer range of 1-2048
priority-value = range of 0-2147483647
```

3.2.2 Command Mode

Configuration mode

3.2.3 Usage

Use `match-list-priority` command to configure the priority for a match-list with the values in the range of 0 to 2147483647.

3.2.4 Examples

```
# configure terminal
(config) #match-list-priority 1 10
```

3.2.5 Validation Commands

`show running-config, show rule match-list`

3.3 match l2param

Use the `match l2param` command to specify L2 parameters that are to be matched.

3.3.1 Command Syntax

`match l2param {dstmac <mac> <mask> | ethertype <ether-value> |innervlan <vlan-id> | srcmac <mac> <mask> | outervlan <vlan-id>}`

`mac` = MAC address in format `HHHH.HHHH.HHHH`

`mask` = MAC address mask in format `HHHH.HHHH.HHHH`

`vlan-id` = VLAN id of range 2-4022

`ether-value` = Range of 0x0000 - 0xFFFF

`dstmac` = To match destination MAC address

`ethertype` = To match ethertype field of the packet. Note that TPID is not to be matched against ethertype.

`innervlan` = To match inner vlan-id in double-tagged packets. This is useful when vlan-stacking is in use.

`srcmac` = To match destination MAC address

`outervlan` = To match VLAN-id in single-tagged packet. In case of double-tagged packet it matches the outer vlan-id.

`no match l2param (dstmac | ethertype | innervlan | srcmac | outervlan)`

3.3.2 Command Mode

Match-list mode

3.3.3 Usage

Use `match l2param` to specify the L2 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L2 parameters to be specified in a single command.

3.3.4 Examples

```
# configure terminal
```

```
(config)# match-list 2 base

(config-mlist)# match l2param dstmac 0080.1111.2222 FFFF.FFFF.FFFF
innervlan 10
```

3.3.5 Validation Commands

`show running-config, show rule match-list`

3.4 match l3param

Use the `match l3param` command to specify L3 parameters that are to be matched. L3 parameters will be working with both L3 and ARP traffic.

3.4.1 Command Syntax

`match l3param {dstip <ipv4-addr> <ipv4-mask> | protocolid <proto-id> | srcip<ipv4-addr> <ipv4-mask>|dscp <0-63> | dstip6 <ipv6-addr> <ipv6-mask> | srcip6 <ipv6-addr> <ipv6-mask>}`

`mask` = IPv4 address mask

`proto-id` = Protocol ID in the IPv4 header or next header value of IPv6 header (next header value of IPv6 extension headers will not be matched)

`dstip` = To match on destination IPv4 address

`protocolid` = To match Protocol-ID in the IPv4 header or next header of IPv6 header (next header of IPv6 extension header will not be matched)

`srcip` = To match on source IPv4 address

`dscp` = To match on DSCP value in the IPv4 or IPv6 header

`dstip6` = To match destination IPv6 address

`srcip6` = To match source IPv6 address

`ipv4-mask` = IPv4 address mask

`ipv6-mask` = IPv6 address mask

`no match l3param (dstip | protocolid | srcip | dscp | dstip6 | srcip6)`

3.4.2 Command Mode

Match-list mode

3.4.3 Usage

Use `match l3param` to specify the L3 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L3 parameters to be specified in a single command.

3.4.4 Examples

```
# configure terminal
(config)# match-list 2 base
(config-mlist)# match l3param dstip 192.168.100.1 255.255.255.255
protocolid 6
```

3.4.5 Validation Commands

`show running-config, show rule match-list`

3.5 match l4param

Use the `match l4param` command to specify L4 parameters that are to be matched.

3.5.1 Command Syntax

`match l4param {l4srcport <portno> (MASK|) |l4dstport <portno> (MASK|)}`

`portno` = Port number of range 0-65535.

`l4dstport` = To match destination port number in L4 header

`l4srcport` = To match source port number in L4 header

`MASK` = Optional portno mask field (given in FFFF format)

`no match l4param {l4dstport | l4srcport}`

3.5.2 Command Mode

Match-list mode

3.5.3 Usage

Use `match l4param` to specify the L4 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L4 parameters to be specified in a single command.

3.5.4 Examples

```
# configure terminal
(config)# match-list 2 base
(config-mlist)# match l4param l4dstport 100 l4srcport 200

# configure terminal
(config)# match-list 3 base
(config-mlist)#match l4param l4srcport 1234 0fff  l4dstport 5678 00ff
```

3.5.5 Validation Commands

`show running-config, show rule match-list`

3.6 match port

Use the `match port` command to specify port parameters that are to be matched.

3.6.1 Command Syntax

`match port ( inports <ports> | srclag <lag-ports> | dstlag <lag-ports> )`
`ports =` Set of ge/xe interface names separated with commas

`lag-ports =` Set of po/sa interface names separated with commas

`inports =` To specify the ports on which the match rule has to be applied. If this is not specified, the rule is applied on all the ports of the chip.

`srclag =` This is to specify that match rule should be applied only if the packet is from a LAG port (Aggregator port), be it static-channel or LACP.

`dstlag =` This is to specify that match rule should be applied only if the packet is destined to a LAG port (Aggregator port), be it static-channel or LACP.

`no match port ( inports | srclag | dstlag )`

3.6.2 Command Mode

Match-list mode

3.6.3 Usage

Use `match port` to specify the port parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters.

3.6.4 Examples

```
# configure terminal
(config)# match-list 2 base
(config-mlist)# match port inports ge1,ge2,ge3
```

3.6.5 Validation Commands

`show running-config, show rule match-list`

3.7 match range

This command qualifies a given match-list for a range of values for a given packet-field. User should specify a valid range ID, otherwise no matching takes place.

3.7.1 Command Syntax

```
match range <range-id>
range-id = 1-64
no match range <1-64>
```

3.7.2 Command Mode

Match-list mode

3.7.3 Example Usage

```
(config)#match-list 1 base
(config-mlist)#match range 10
```

3.7.4 Validation Commands

`show range, show running-config range`

3.8 match udf

This command is used to mention the specific data and mask, which need to be matched in a given packet. The data and mask accept 4-byte values for the base UDFs and 2-byte values for the fabric UDFs. To match a particular UDF, it must already been created using `set udf` command. For creating UDF, see *udf <0-15> on page 165*.

3.8.1 Command Syntax

`match udf <0-15> <data> <mask>`

`udf-id = 0-15`

`data =` Data pattern to match

`mask =` Mask pattern

3.8.2 Command Mode

Match-list mode

3.8.3 Example Usage

```
(config)#match-list 257 base
(config-egress-mlist)#match udf 1 0x11111111 0xffffffff
```

3.8.4 Validation Commands

`show running-config udf, show udf`

3.9 range

This command creates a range, identified by the given range ID, for a specific packet field. The range IDs 1-32 are reserved for the base chipset and 33-64 are reserved for the fabric chipset. The fields on which the range checker is applied are Layer 4 source port, Layer 4 destination port,and Outer-Vlan Id. The range has to be supplied with a minimum value and a maximum value. These values cannot exceed 65535.

3.9.1 Command Syntax

`range <range-id> <range-type> <min> <max>`

`range-id` = 1-64

`range-type` = l4srcport|l4dstport|outervlan

`min` = Minimum value for the range

`max` = Maximum value for the range

`no range <1-64>`

3.9.2 Command Mode

Configuration mode

3.9.3 Example Usage

```
(config)#range 1 l4srcport 100 200
```

3.9.4 Validation Commands

`show range, show running-config range`

3.10 rule match-list

Use the `rule match-list` command to apply an action based on the specified match-list.

3.10.1 Command Syntax

`rule match-list <match-list-ids> action { redirect-port <ports> | redirectlag <lag-port>| drop | mirror-ingress <port> | mirror-egress <port> |modify-vlanid <vlan-id> | modify-pktpriority <priority> | modify-dstmac<MAC> | modify-dscp <dscp> | copytocpu | egress-mask <port> | modify-IntPriority <priority> | tos-as-priority | modify-pktIntPriority<priority> | update-counters <counters> }`

`match-list-id` = Range of 1-2048

`port` = Interface name

`ports` = Interface names separated by commas

`lag-port =` LAG interface (po or sa)

`vlan-id =` Range 2-4022.

`priority =` Range of 0-7

`tos =` 0-7

`dscp =` 0-63

`counters =` lower | upper | red_notred | green_notgreen | green_red | green_yellow | red_yellow

All the rules are applied on the matched packets based on the specific match rule.

`redirect-port =` To redirect the matched packets to port(s) irrespective of the VLAN settings. The port(s) can be ge# or xe# or higig.

`redirect-lag =` To redirect the matched packets to a specific LAG interface (sa/po)

`drop =` To drop the matched packets and not forward

`mirror-ingress =` To mirror matched packets at ingress

`mirror-egress =` To mirror matched packets at egress

`modify-vlanid =` To modify VLAN-tag in the matched VLAN-tagged packets

`modify-pktpriority =` To modify priority in the 802.1Q tag header

`modify-dstmac =` To modify destination MAC address in the matched packets

`modify-dscp =` To modify DSCP field in the IP header

`copytocpu =` To forward the matched packets to the CPU port

`egress-mask =` To specify the list of ports on which the matched packet should not be forwarded

`modify-IntPriority =` To direct the matched packets to a priority queue of the switch. This does not modify priority field in the 802.1Q tag header.

`tos-as-priority =` To modify priority in 802.1Q tag header to the value in TOS field of IP headerIPv4 header or to the value of Traffic class field in IPv6 header.

`modify-pktIntPriority =` To modify priority in 802.1Q tag header and to direct the matched packets to a priority queue of the switch.

`update-counters =` To update the counters based on the Diffserv code points

3.10.2 Command Mode

Configure mode

3.10.3 Usage

Use `rule match-list` to control transmission of packets or modify the packets. This command is used to specify the actions to be performed if a packet matches with the match-list specified. This command allows to configure multiple actions for multiple match-lists.

3.10.4 Examples

```
# configure terminal
(config) # rule match-list 2,4 action modify-vlanid 10 modify-dscp 30
(config) # rule match-list 2-5 action modify-vlanid 10 modify-dscp 30
```

3.10.5 Validation Commands

`show running-config, show rule match-list`

For sample output of the validation commands, refer Appendix A *rule match-list on page 254*.

The Filter Process Rule Modify Vlan-Id is applied after L2 Forwarding. So, egress port should be added to the same VLAN of the actual traffic for successful L2 Forwarding. In addition to the actual traffic Vlan-Id, the egress port should also be added to the modified Vlan-Id for the traffic to pass the egress filtering rules.

3.11 set udf

This command is used to set the UDFs in the hardware once all the UDFs are created for the corresponding chipset. Once this command is executed, the UDFs cannot be modified for this chipset; user needs to unset the field using "no udf database" and create the UDFs again.

3.11.1 Command Syntax

```
set udf <unit> enable
unit = base|fabric
```

3.11.2 Command Mode

UDF database mode

3.11.3 Example Usage

```
(config)# udf database base
(config-udf)#set udf base enable
```

3.11.4 Validation Commands

```
show running-config udf, show udf
```

3.12 show match-list pending

Use this command to display match-list(s) that are not yet installed.

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, SRstackware CLI Environment on page 41*.

3.12.1 Command Syntax

```
show match-list pending [<match-list-id>]
```

3.12.2 Command Mode

Privileged Exec Mode

3.12.3 Usage

The following is a sample output of the show match-list pending command showing the match-list entries that are not yet installed.

```
# show match-list pending
match-list 1
  match l3param protocolid 3
match-list 2
  match l2param innervlan 44
```

3.12.4 Examples

```
# show match-list pending
# show match-list pending 2
```

3.13 show range

This command displays the range entries configured currently on the device.

3.13.1 Command Syntax

`show range (<range-id>)`

`range-id = 1-64`

3.13.2 Command Mode

Exec mode

3.13.3 Example Usage

`#show range 10`

3.14 show rule match-list

Use this command to display match-list(s).

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, SRstackware CLI Environment on page 41*.

3.14.1 Command Syntax

`show rule match-list (match-list-id)`

`match-list-id = Range 1-1792`

3.14.2 Command Mode

Privileged Exec mode

3.14.3 Usage

The following is a sample output of the `show rule match-list` command showing the match-list entries.

`#show rule match-list <1-2048>`

3.14.4 Examples

```
# show rule match-list
# show rule match-list 2
```

3.15 show running-config range

This command displays the configuration of all the range checkers currently configured on the device.

3.15.1 Command Syntax

```
show running-config range
```

3.15.2 Command Mode

Privileged Exec mode

3.15.3 Example Usage

```
#show running-config range
```

3.16 show running-config udf

This command displays the configuration of all the UDFs present on the device.

3.16.1 Command Syntax

```
show running-config udf
```

3.16.2 Command Mode

Privileged Exec mode

3.16.3 Example Usage

```
#show running-config udf
```

3.17 show udf (<0-15>)

This command displays a particular or entire UDF configuration on the device.

3.17.1 Command Syntax

```
show udf <udf-id>
udf-id = 0-15
```

3.17.2 Command Mode

Privileged Exec mode

3.17.3 Example Usage

```
#show udf 1
#show udf
```

3.18 udf <0-15>

This command is used to create user-defined fields. The various parameters of the this command correspond to the parameters of UDF. The IDs 0-7 are valid for the base chipset and the IDs 8-15 are valid for the fabric chipset.

3.18.1 Command Syntax

```
udf <0-15> vlan <tag> ip <ip-type> <offset-value>

tag = no-tag | 1-tag | 2-tag
ip-type = ip4hdronly | ip6hdronly | ip4overip4 | ip6overip4 | ip4overip6
|ip6overip6 | greip4overip4 | greip6overip4 | greip4overip6 |
greip6overip6 | onemplslabel | twomplslabels | ipnotused
offset-value = 0-31

no udf <0-15>
```

Parameter	Description
`tag`	The VLAN parameter specifies the presence of tag for the packets that to be matched.
`ip-type`	The IP parameter specifies type of IP header that the packets to be matched.
`offset-value`	The offset parameter specifies which chunk (set of bytes) to be matched in the packet.

Offset table for base chipset:

Chunk 0	Chunk 1	Chunk 2	…….	Chunk 29	Chunk 30	Chunk 31
B126, B127, B0, B1	B2-B5	B6-B9	…….	B114-B117	B118-B121	B122-B125

Offset table for fabric chipset:

Chunk 0	Chunk 1	Chunk 2	…….	Chunk 29	Chunk 30	Chunk 31
B0, B1	B2, B3	B4, B5	…….	B58, B59	B60, B61	B62, B63

NOTICE

The IP type "ipnotused" works only for L2 packets; it does not match packets with MPLS headers.

The ethertype value for vlan 1-tag and 2-tag options must be 0x8100.

3.18.2 Command Mode

UDF database mode

3.18.3 Example Usage

```
(config)#udf database base
(config-udf)#udf 1 vlan no-tag ip ip4hrdonly 5

(config)#udf database fabric
(config-udf)#udf 10 vlan 1-tag ip ip6hdronly 10
```

3.18.4 Validation commands

```
show running-config udf, show udf
```

3.19 udf database

This command switches the system to UDF database mode where user can create user-defined fields and enable the fields on the corresponding chipset. Once the UDFs are enabled on a particular chipset, they cannot be modified. User needs to unset the fields using the no command (as shown in the Command Syntax) and recreate the UDFs.

3.19.1 Command Syntax

```
udf database <unit>
unit = base|fabric
no udf database (base|fabric)
```

3.19.2 Command Mode

Configuration mode

3.19.3 Example Usage

```
(config)#udf database base
(config-udf)#
```

3.19.4 Validation Commands

```
show running-config udf, show udf
```

VLAN match-list Commands

4.1 Overview

Pre-Ingress/Vlan Match-lists are the initial stages of filter entries in the hardware's filter processor engine. The vlan stage of the filter processor is followed by (Ingress) Match-lists and than Egress match-lists.

4.2 vlan-match-list

Use the `vlan-match-list` command to configure a match-list for performing various actions on the matched packets in the pre-ingress/vlan stage of the filter processor.

4.2.1 Command Syntax

```
vlan-match-list (<1-512>|<513-1024>) (base|fabric)
```

4.2.2 Command Mode

Configure mode

4.2.3 Usage

This command takes the system to pre-ingress/vlan Match-list mode where the user can specify various parameters to match the packets that flow through pre-ingress pipe-line of the specified unit. The vlan match-list IDs 1-512 are reserved for the base unit and 513-1024 are fixed for the fabric unit.

4.2.4 Examples

```
#configure mode
(config)#vlan-match-list 1 base
(config-vlan-mlist)#
```

4.2.5 Validation Commands

```
show running-config, show rule vlan-match-list
```

4.3 vlan-match-list-priority

A priority can be assigned to each individual vlan match-lists by making the higher prioritized match-list to be matched first among all the possible matches.

4.3.1 Command Syntax

`vlan-match-list-priority <1-1024> <0-2147483647>`

`vlan-match-list-id =` Integer range of 1 - 1024

`priority-value =` Range of 0 - 2147483647

4.3.2 Command Mode

Configuration mode

4.3.3 Usage

Use `vlan-match-list-priority` command to configure the priority for a vlan-match-list with the values in the range of 0 to 2147483647.

4.3.4 Examples

```
#configure mode
(config)#vlan-match-list-priority 1 10
```

4.3.5 Validation Commands

`show running-config, show rule vlan-match-list`

4.4 match l2param

Use the `match l2param` command to specify L2 parameters that are to be matched with the vlan match-list entries.

4.4.1 Command Syntax

`match l2param {dstmac <MAC> <MASK>|srcmac <MAC> <MASK>|ethertype <ETHER-VALUE>| outervlan-id <VLAN-ID>| outervlan-cfi <CFI-BIT>| outervlan-priority <PRIORITY>}`

`MAC` = MAC address in format `HHHH.HHHH.HHHH`

`MASK` = MAC address mask in format `HHHH.HHHH.HHHH`

`VLAN-ID` = VLAN id of range 2-4022

`ETHER-VALUE` = Range of 0x0000 - 0Xffff

`CFI-BIT` = CFI bit value 0 or 1

`dstmac` = To match destination MAC address

`srcmac` = To match source MAC address

`ethertype` = To match ethertype field of the packet. Note that TPID is not to be matched against ethertype.

`outervlan-cfi` = To match CFI bit value in the outer vlan tag

`outervlan-priority` = To match 802.1p priority value in the outer vlan tag

`no match l2param (dstmac| srcmac| ethertype| outervlan-id| outervlan-cfi| outer-vlan-priority)`

4.4.2 Command Mode

Vlan-match-list mode

4.4.3 Usage

Use `match l2param` command to specify the L2 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L2 parameters to be specified in a single command.

4.4.4 Examples

```
(config)#vlan-match-list 1 base
(config-vlan-mlist)#match l2param ethertype 0x8100 outervlan-id 95
outervlan-priority 7
(config-vlan-mlist)#no match l2param ethertype
```

4.4.5 Validation Commands

`show running-config, show rule vlan-match-list`

4.5 match l3param

Use the `match l3param` command to specify L3 parameters that are to be matched with the vlan match-list entries. L3parameters will be working with both L3 and ARP traffic.

4.5.1 Command syntax

```
match l3param {srcip <IPv4-ADDR> <MASK>|dstip <IPv4-ADDR> <MASK>
|protocolid <PROTO-ID>| dscp <DSCP-VALUE>}
```

`srcip` = To match on source IPv4 address

`dstip` = To match on destination IPv4 address

`IPv4-ADDR` = IPv4 Address

`MASK` = IPv4 Address mask

`protocolid` = To match protocol ID in the IPv4 address

`PROTO-ID` = Protocol ID in the IPv4 header

`dscp` = To match DSCP in the IPv4 address

`DSCP-VALUE` = DSCP value in the IPv4 header

```
no match l3param {srcip| dstip| protocolid| dscp}
```

4.5.2 Command Mode

Vlan-match-list mode

4.5.3 Usage

Use `match l3param` to specify the L3 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L3 parameters to be specified in a single command.

4.5.4 Examples

```
(config)#vlan-match-list 1 base
(config-vlan-mlist)#match l3param srcip 192.168.1.1 255.255.255.255
protocolid 6
(config-vlan-mlist)#no match l3param protocolid
```

4.5.5 Validation Commands

`show running-config, show rule vlan-match-list`

4.6 match l4param

Use the `match l4param` command to specify L4 parameters that are to be matched with the vlan match-list entries.

4.6.1 Command Syntax

`match l4param {l4srcport <portno> (MASK|) |l4dstport <portno>(MASK|)}`

`portno` = Port number of range 0-65535

`l4dstport` = To match destination port number in L4 header

`l4srcport` = To match source port number in L4 header

`MASK` = Optional portno mask field (given in FFFF format)

`no match l4param {l4dstport | l4srcport}`

4.6.2 Command Mode

Vlan-match-list

4.6.3 Usage

Use `match l4param` to specify the L4 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use no command to delete the matched parameters. This command accepts multiple L4 parameters to be specified in a single command.

4.6.4 Examples

```
(config)#vlan-match-list 1 base
(config-vlan-mlist)#matchl4param l4srcport 1234 0fff l4dstport 5678 00ff
```

4.6.5 Validation Commands

`show running-config, show rule vlan-match-list`

4.7 rule vlan-match-list

Use the `rule vlan-match-list` command to apply an action based on the specified vlan-match-list.

4.7.1 Command Syntax

`rule vlan-match-list <VLAN-MLIST-ID> action {drop| modify-outer-vlanid <VLAN-ID>| modify-pktpriority <PRIO>|modify-IntPriority <PRIO>| copytocpu| dont-learn| drop-precedence <DP>| delete-inner-vlan| modify-inner-vlanid <VLAN-ID>| add-inner-vlanid <VLAN-ID>| add-outer-vlanid <VLAN-ID>}`

`VLAN-MLIST-ID` = match-list ID in the range of 1-1024

`VLAN-ID` = Vlan ID in the range of 2-4022

`PRIO` = Priority value in the range of 0-7

`DP` = Drop precedence with the values of GREEN, YELLOW and RED

`drop` = To drop the matched packet and not to forward

`modify-outer-vlanid` = To modify VLAN-tag in the matched VLAN-tagged packets

`modify-pktpriority` = To modify priority in the 802.1Q tag header

`modify-IntPriority` = To direct the matched packets to a priority queue of the switch.This does not modify priority field in the 802.1Q tag header.

`copytocpu` = To forward the matched packets to CPU port

`dont learn` = Not to learn the source MAC of the matched packets

`drop-precedence` = To assign drop-precedence to the matched packets

`delete-inner-vlan` = To delete the inner VLAN Tag of the matched packets, if it has more than one VLAN tag

`modify-inner-vlanid` = To modify inner VLAN-tag in the matched VLAN-tagged packets, if it has more than one VLAN tag

`add-inner-vlanid` = To append an inner VLAN-tag in the matched packets

`add-outer-vlanid` = To append an outer VLAN-tag in the matched packets

`no rule vlan-match-list <VLAN-MLIST-ID>`

4.7.2 Command Mode

Configuration mode

4.7.3 Usage

Use `rule match-list` command to control transmission of packets or modify the packets. This command is used to specify the actions to be performed if a packet matches with the matchlist specified. This command allows to configure multiple actions for multiple match-lists.

4.7.4 Examples

```
(config)#rule vlan-match-list 1 action dont-learn modify-outer-vlanid 10
(config)#no rule vlan-match-list 1
```

4.7.5 Validation Commands

`Show running-config`

4.8 show rule vlan-match-list

Use this command to display the set of vlan match-list(s) that are currently installed.

4.8.1 Command Syntax

`show rule vlan-match-list (match-list-id)`

`match-list-id =` VLAN match-list ID in the range of 1-1024

4.8.2 Command Mode

Privileged Exec mode

4.8.3 Usage

The following is the sample output of show rule vlan-match-list command showing the vlan-match-list entries.

```
#show rule vlan-match-list
vlan-match-list 1000 fabric
```

```
  L2 params:
    outervlan-id 91
  Actions:
    modify-outer-vlanid 92
vlan-match-list 1001 fabric
  L2 params:
    ethertype 0x8100
  L3 params:
    dscp 56
  L4 params:
    l4dstport 23
  Actions:
    modify-pktpriority 6
    modify-outer-vlanid 91
    dont-learn
```

4.8.4 Examples

```
#show rule vlan-match-list
#show rule vlan-match-list 1001
```

4.9 show vlan-match-list pending

Use this command to display vlan-match-list(s) that are not yet installed.

4.9.1 Command Syntax

```
show vlan-match-list pending
```

4.9.2 Command Mode

Privilege Exec mode

4.9.3 Usage

The following is the sample output of show vlan-match-list pending command showing uninstalled vlan-match-list entries.

```
#show vlan-match-list pending
vlan-match-list 200 base
  match l2param outervlan-cfi 1 outervlan-priority 4
  match l3param dscp 63
  match l4param l4dstport 20
vlan-match-list 300 base
  match l3param srcip 192.168.24.100 255.255.255.0
  match l4param l4srcport 19
```

4.9.4 Examples

```
#show vlan-match-list pending
```

Egress match-list

5.1 Overview

Egress Match-lists is the last stage of filter entries in the hardware's filter processor engine. The egress stage of the filter processor is preceded by Vlan Match-lists and (ingress)match-lists in the order.

5.2 egress-match-list

Use the `egress-match-list` command to configure a match-list for performing various actions on the matched packets in the egress stage of the filter processor.

5.2.1 Command Syntax

```
egress-match-list (<1-256>|<257-786>) (base|fabric)
```

5.2.2 Command Mode

Configuration mode

5.2.3 Usage

This command takes the system to Egress Match-list mode where the user can specify various parameters to match the packets that flow through egress pipe-line of the specified unit. The egress match-list IDs 1-256 are reserved for the base unit and 257-768 are fixed for the fabric unit.

5.2.4 Examples

```
(config)#egress-match-list 1 base
(config-egress-mlist)#
```

5.2.5 Validation Commands

`show running-config, show egress rule match-list.`

5.3 egress-match-list-priority

A priority can be assigned to each individual egress match-lists by making the higher prioritized match-list to be matched first among all the possible matches.

5.3.1 Command Syntax

`egress-match-list-priority <1-768> <0-2147483647>`

5.3.2 Command Mode

Configuration mode

5.3.3 Usage

User can configure the priority of a Match-list with the values in the range of 0 to 2147483647. An error will be thrown if the given Match-list ID is not yet installed in the hardware.

5.3.4 Examples

`#egress-match-list-priority 1 10`

5.3.5 Validation Commands

`show running-config, show egress rule match-list.`

5.4 match l2param

Use the `match l2param` command to specify L2 parameters that are to be matched with the egress match-list entries.

5.4.1 Command Syntax

`match l2param {dstmac MAC MASK|srcmac MAC MASK|ethertype VALUE| outervlan VLAN-ID}`

`MAC` = MAC address in format `HHHH.HHHH.HHHH`

`MASK` = MAC address mask in format `HHHH.HHHH.HHHH`

`VLAN-ID` = VLAN id of range 2-4022

`ETHER-VALUE` = Range of 0x0000 - 0Xffff

`dstmac` = To match destination MAC address

`srcmac` = To match source MAC address

`ethertype` = To match ethertype field of the packet. Note that TPID is not to be matched against ethertype

`outervlan` = To match VLAN-id in single-tagged packet. In case of double-tagged packets it matches the outer vlan-id

`no match l2param {dstmac | srcmac | ethertype | outervlan}`

5.4.2 Command Mode

Egress match-list mode

5.4.3 Usage

Use this command to specify various Layer 2 packet parameters and their values based on which the packets must be matched and actions are to applied to control the transmission of packets. This command allows multiple parameters to be specified in the single command.

5.4.4 Examples

```
(config)#egress-match-list 1 base
(config-egress-mlist)#match l2param outervlan 100
```

5.4.5 Validation Commands

`Show running-config, show egress rule match-list`

5.5 match l3param

Use the `match l3param` command to specify L3 parameters that are to be matched with the egress match-list entries. L3 parameters will be working with both L3 and ARP traffic.

5.5.1 Command Syntax

```
match l3param {srcip <IPv4-ADDR> <MASK>|dstip <IPv4-ADDR> <MASK>
|protocolid <PROTO-ID>}
```

`IPv4-ADDR` = IPv4 Address

`MASK` = IPv4 Address mask

`PROTO-ID` = Protocol ID in the IPv4 header

`srcip` = To match on source IPv4 address

`dstip` = To match on destination IPv4 address

`protocolid` = To match protocol ID in the IPv4 address

```
no match l3param {srcip| dstip| protocolid}
```

5.5.2 Command Mode

Egress match-list mode

5.5.3 Usage

Use `match l3param` to specify the L3 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L3 parameters to be specified in a single command.

5.5.4 Examples

```
(config)#egress-match-list 1 base
(config-egress-mlist)#match l3param srcip 192.168.1.1 255.255.255.255
protocolid 6
(config-egress-mlist)#no match l3param protocolid
```

5.5.5 Validation Commands

`show running-config, show egress rule match-list`

5.6 match l4param

Use the `match l4param` command to specify L4 parameters that are to be matched with the egress match-list entries.

5.6.1 Command Syntax

`match l4param {l4srcport <portno> (MASK|) |l4dstport <portno> (MASK|)}`

`portno =` Port number of range 0-65535.

`l4dstport =` To match destination port number in L4 header

`l4srcport =` To match source port number in L4 header

`MASK =` Optional portno mask field (given in FFFF format)

`no match l4param {l4dstport | l4srcport}`

5.6.2 Command Mode

Egress match-list

5.6.3 Usage

Use `match l4param` to specify the L4 parameters and their values based on which the actions are applied to control the transmission of packets and update various contents in the packets. Use `no` command to delete the matched parameters. This command accepts multiple L4 parameters to be specified in a single command.

5.6.4 Examples

```
(config)#egress-match-list 1 base
(config-egress-mlist)#matchl4param l4srcport 1234 0fff l4dstport 5678
00ff
```

5.6.5 Validation Commands

`show running-config, show egress rule match-list`

5.7 egress rule match-list

Use the `egress rule match-list` command to apply an action or set of actions to the specified egress match-list entry.

5.7.1 Command Syntax

`egress rule match-list VALUE action {drop| modify-vlanid VLAN-ID| modify-pktpriority PRIO| modify-dscp DSCP}`

`VALUE` = Match-list ID in the range of 1-768

`VLAN-ID` = Vlan ID in the range of 2-4022

`PRIO` = Priority value in the range of 0-7

`DSCP` = DSCP value in the range of 0-63

`drop` = To drop the matched packets and do not forward

`modify-vlanid` = To modify the outer VLAN tag of the matched packet, if it has at least one VLAN tag

`modify-vlanpriority` = To modify the priority in 802.1Q header

`modify-dscp` = To modify DSCP value in the IPv4 header

`no egress rule match-list VALUE`

5.7.2 Command Mode

Configuration mode

5.7.3 Usage

This command is used to specify actions that are to be performed if a packet matches with the corresponding egress match-list. This command allows multiple actions to be specified.

5.7.4 Examples

```
(config)#egress rule match-list 1 action drop modify-vlanid 10 modify-dscp 10
(config)#no egress rule match-list 1
```

5.7.5 Validation Commands

```
Show running-config, show egress rule match-list
```

5.8 show egress rule match-list

Use this command to display the set of egress match-list(s) that are currently installed.

5.8.1 Command Syntax

```
show egress rule match-list  (<1-768>)
```

5.8.2 Command Mode

Privileged Exec mode

5.8.3 Usage

This command is used to display the list of egress match-lists that are installed in the hardware.

5.8.4 Examples

```
#show egress rule match-list
#show egress rule match-list 5
```

5.9 show egress-match-list pending

Use this command to display the list of egress match-list(s) that are not yet installed.

5.9.1 Command Syntax

```
show egress-match-list pending
```

5.9.2 Command Mode

Privileged Exec mode

5.9.3 Usage

This command dispalys the list of egress match-lists that are not yet installed.

5.9.4 Examples

```
#show egress-match-list pending
```

QoS Commands

6.1 Overview

This chapter contains QoS commands in alphabetical order. These commands are available only if SRstackware is compiled with the `--enable-qos` configuration option.

6.2 class

Use this command to define a traffic classification. Use the `no` parameter with this command to delete an existing class-map.

6.2.1 Command Syntax

```
(no) class NAME
```

`NAME` = Name of the class map.

6.2.2 Command Mode

Policy Map mode

6.2.3 Example

The following example shows creating a policy map, and defining the traffic classification.

```
# configure terminal
(config)# policy-map pmap1
(config-pmap)# class cmap1
```

6.2.4 Related Commands

`class-map, policy-map`

6.3 class-map

Use this command to create a class map. Use the `no` parameter with this command to delete an existing class-map.

6.3.1 Command Syntax

`(no) class-map NAME`

`NAME` = Name of the class map

6.3.2 Command Mode

Configure mode

6.3.3 Example

The following example shows creating a class map.

```
# configure terminal
(config)# class-map cmap1
```

6.3.4 Related Commands

`class, policy-map, show class-map`

6.4 ip-access-list

Use this command to create an IP access-control list (ACL) based on the source address, or create an IP extended ACL based on the source and destination address. Use the no parameter with this command to delete an IP, or IP extended ACL.

6.4.1 Command Syntax

The following syntax creates an IP ACL based on the source address:

`(no) ip-access-list ACCESS-LIST NUMBER deny|permit SOURCE (SOURCE WILDCARD)`

`ACCESS-LIST NUMBER`

`<1-99>` = Range for IP standard ACL

`<1300-1999>` = Expanded range for IP standard ACL

`deny` = Deny certain traffic if conditions matched

`permit` = Permit certain traffic if conditions matched

SOURCE = Originating network or host sending packet. If the mask is set to 255.255.255.255, the specified source address is ignored, and can be replaced by the word, any. For example, `ip-access-list 10 permit 0.0.0.0 255.255.255.255` and `ip-access-list 10 permit 33.44.11.34 255.255.255.255` can be replaced by `ip-access-list 10 permit any`.

SOURCE WILDCARD = Optional. Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.

The following syntax creates an IP extended ACL based on the source and destination address:

`(no) ip-access-list ACCESS-LIST NUMBER deny|permit ip SOURCE (SOURCE WILDCARD) DESTINATION (DESTINATION WILDCARD)`

ACCESS-LIST NUMBER

<100-199> = Range for IP extended ACL

<2000-2699> = Expanded range for IP extended ACL

deny = Deny certain traffic if conditions matched

permit = Permit certain traffic if conditions matched

SOURCE = Originating network or host sending packet. Can be A.B.C.D, host, or any. The host keyword can be used for host IP addresses (where the mask is 0.0.0.0). For example, `ip-access-list 10 permit 2.2.2.2 0.0.0.0` can be replaced by `ip-access-list 4 permit host 2.2.2.2`.

SOURCE WILDCARD = Optional. Wildcard bits in dotted decimal notation to apply to the source. Ones go in bit positions to ignore.

DESTINATION = Destination IP address. Can be A.B.C.D, host, or any.

DESTINATION WILDCARD = Optional. Wildcard bits in dotted decimal notation to apply to the destination. Ones go in bit positions to ignore.

6.4.2 Command Mode

Configure mode

6.4.3 Example

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

```
# configure terminal
(config)# ip-access-list 1 permit 192.5.255.0 0.0.0.255
(config)# ip-access-list 1 permit 128.88.0.0 0.0.255.255
(config)# ip-access-list 1 permit 36.0.0.0 0.0.0.255
```

6.5 mac-access-list

Use this command to create a MAC ACL. Use the no parameter with this command to delete a MAC ACL.

6.5.1 Command Syntax

`(no) mac-access-list <2000-2699> deny|permit SRC_MAC MASK DEST_MAC MASK <1-8>`

`<2000-2699>` Range for MAC ACL

deny = Deny certain traffic if conditions matched

`permit` = Permit certain traffic if conditions matched

`SRC_MAC` = Source MAC address; in `HHHH.HHHH.HHHH` format

`DEST_MAC` = Destination MAC address; in `HHHH.HHHH.HHHH` format

`MASK` = Specify which part of the MAC address will be ignored. In hexadecimal format

any = can replace either the `SRC_MAC MASK` pair or the corresponding `DEST_MAC MASK` pair, but not both pairs.

`<1-8>` = Specify packet format. For example, 1 for Ethernet II, 2 for 802.3, 8 for LLC

6.5.2 Command Mode

Configure mode

6.5.3 Example

```
# configure terminal
(config)# mac-access-list 2002 permit 2222.2222.2222 0000.0000.0000
1111.1111.1212 0000.0000.0000 8
```

6.6 mac-access-list priority

Use this command to set the priority of the source or destination MAC. Use the no parameter with this command to remove the entry.

6.6.1 Command Syntax

`(no) mac-access-list <2000-2699> source|destination MAC priority <0-7>`

`<2000-2699>` = MAC access list number

`source` = Priority of source MAC

`destination` = Priority of destination MAC

`MAC` = MAC address, in `HHHH.HHHH.HHHH` format

`<0-7>` = Priority value

6.6.2 Command Mode

Configure mode

6.6.3 Example

```
# configure terminal
(config)# mac-access-list 2002 source 2222.2222.2222 priority 2
```

6.7 match access-group

Use this command to define match criterion for a class map.

6.7.1 Command Syntax

`match access-group NAME`

`NAME` = Number of name of the ACL

6.7.2 Command Mode

Class Map mode

6.7.3 Example

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

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

6.7.4 Related Commands

`class-map`

6.8 match ip-dscp

Use this command to define the list to match against incoming packets.

6.8.1 Command Syntax

match ip-dscp LIST

`LIST` = List to match against incoming packets. Up to 8 IP DSCP values separated by a space. Range is 0-63.

6.8.2 Command Mode

Class Map mode

6.8.3 Usage

Use the match ip-dscp command to define the match criterion after creating a class map.

6.8.4 Example

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

```
# configure terminal
(config)# class-map cmap1
(config-cmap)# match ip-dscp 56
```

6.8.5 Related Commands

`class-map, match vlan-range`

6.9 match ip-precedence

Use this command to identify IP precedence values as match criteria. Use the no parameter with this command to remove IP precedence values from a class map.

6.9.1 Command Syntax

`(no) match ip-precedence VALUE`

`VALUE <0-7>` = Specifies the exact value from 0 to 7 used to identify a precedence value. Can be up to 8 precedence values.

6.9.2 Command Mode

Class Map mode

6.9.3 Example

The following example shows configuring a class-map named cmap1 to evaluate all IPv4 packets for a precedence value of 5.

```
(config)# class-map cmap1
(config-cmap)# match ip-precedence 5 6 4 3
```

6.10 match layer4

Use this command to identify UDP or TCP ports as the match criteria. Use the no parameter with this command to remove the match criteria.

6.10.1 Command Syntax

`(no) match layer4 source-port|destination-port <1-65535>`

`source-port` = Source UDP or TCP port. Range is 1-655535

`destination-port` = Destination UDP or TCP port. Range is 1-655535

6.10.2 Command Mode

Class Map mode

6.10.3 Example

```
(config)# class-map cmap1
(config-cmap)# match layer4 source-port 20
```

6.11 match mpls exp-bit topmost

Use this command to define the match criterion of the MPLS experimental bit value in the topmost label for a class map. Use the `no` parameter with this command to remove this criterion from a class map.

6.11.1 Command Syntax

`(no) match mpls exp-bit topmost <0-7>`

`<0-7>` = Experimental value. Can be up to 8 values.

6.11.2 Command Mode

Class Map mode

6.11.3 Example

The following example shows configuring a class-map named cmap1 with criterion that matches MPLS experimental bit, 0 1 2 3 4 5 6 7.

```
(config)# class-map cmap1
(config-cmap)# match mpls exp-bit topmost 0 1 2 3 4 5 6 7
```

6.12 match vlan

Use this command to define the VLAN ID used as match criteria to classify a traffic class. Use the no parameter with this command to disable the VLAN ID used as match criteria.

6.12.1 Command Syntax

```
(no) match vlan <1-4022>
```

6.12.2 Command Mode

Class Map mode

6.12.3 Example

The following example shows configuring a class-map named cmap1 to include traffic from VLAN 3.

```
(config)# class-map cmap1
(config-cmap)# match vlan 3
```

6.13 match vlan-range

Use this command to specify the range of VLANs for classifying traffic on a per-port-per-VLAN basis.

6.13.1 Command Syntax

```
match vlan-range <2-4022> to <2-4022>
```

6.13.2 Command Mode

Class Map mode

6.13.3 Usage

Use the `match vlan-range` command to specify the range of VLANs after defining the match criterion, and creating a class map when classifying traffic on a per-port-per-VLAN basis.

6.13.4 Example

The following example shows configuring a class map named cmap1 with criterion that matches IP DSCP 56, with a VLAN range of 20 to 30.

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

6.13.5 Related Commands

`class-map, match ip-dscp`

6.14 mls qos

Use this command to globally enable QoS, and define queueing. Use the `no` parameter with this command to globally disable QoS.

6.14.1 Command Syntax

`(no) mls qos QUEUE_WEIGHT COS_VALUE`

`QUEUE_WEIGHT` = Weight of each of the 8 egress queues; range is 0-10

`COS_VALUE CoS` = Values mapped to each of the 8 egress queues; range is 0-7

The following describes a stub command used in non-standard configurations. In this case, this command is used to globally enable or disable QoS without defining queueing.

`(no) mls qos`

6.14.2 Command Mode

Configure mode

6.14.3 Example

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

6.15 mls qos aggregate-police

Use this command to specify policer parameters to apply to multiple traffic classes in the same policy map. Use the no parameter with this command to delete an aggregate policer, along with its parameters.

6.15.1 Command Syntax

`(no) mls qos aggregate-police NAME RATE BURST exceed-action drop`

`NAME` = Name of the aggregate policer

`RATE` = Average traffic rate in bits per second (bps). Range is 1-1000000

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

`exceed-action drop` = Specify dropping the packet when rates are exceeded

6.15.2 Command Mode

Configure mode

6.15.3 Example

The following example shows specifying policer parameters with a traffic rate of 48000 bps and a burst size of 8000 bps.

```
# configure terminal
(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action drop
```

6.15.4 Related Commands

`police-aggregate, show mls qos aggregate policer`

6.16 mls qos map dscp-cos

Use this command to create a DSCP-to-CoS map. Use the no parameter with this command to remove a configured DSCP-to-CoS mapping table.

6.16.1 Command Syntax

`(no) mls qos map dscp-cos UNIT-NAME LIST to VALUE`

`UNIT-NAME` = Name of unit

`LIST` = Up to 8 DSCP values, each separated by a space. Range is 0-63.

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

6.16.2 Command Mode

Configure mode

6.16.3 Example

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

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

6.16.4 Related Commands

`show mls qos maps dscp-cos`

6.17 mls qos map dscp-mutation

Use this command to modify the DSCP-to-DSCP mutation map. Use the `no` parameter with this command to return to the default map.

6.17.1 Command Syntax

`(no) mls qos map dscp-mutation UNIT_NAME IN_DSCP to OUT_DSCP`

`UNIT_NAME` = Name of unit

`IN_DSCP` = 8 DSCP values separated by spaces; range is 0-63

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

6.17.2 Command Mode

Configure mode

6.17.3 Example

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

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

6.17.4 Related Commands

`show mls qos maps dscp-mutation`

6.18 mls qos min-reserve

Use this command to specify the minimum reserve-level and buffer size on all Ethernet ports. Use the no parameter with this command to return to the default minimum reserve buffer size.

6.18.1 Command Syntax

`(no) mls qos min-reserve <1-8> <10-170>`

`<1-8>` = Minimum-reserve level

`<10-170>` = Minimum-reserve buffer size, in packets

6.18.2 Command Mode

Configure mode

6.18.3 Default

The buffer size for all minimum-reserve levels is 0 packets.

6.18.4 Example

The following example shows configuring minimum-reserve level 4 to 21 packets.

```
# configure terminal
(config)# mls qos min-reserve 4 21
```

The following example shows configuring minimum-reserve level 4 to 21 packets, and assigning minimum-reserve level 4 to egress queue 2 on interface, fe1.

```
# configure terminal
(config)# mls qos min-reserve 4 21
(config)# interface fe1
(config-if)# wrr-queue min-reserve 2 4
```

6.18.5 Related Commands

`wrr-queue min-reserve`

6.19 police

Use this command to specify a policer. Use the `no` parameter with this command to remove an existing policer.

6.19.1 Command Syntax

`(no) police RATE BURST exceed-action drop`

`RATE` = Average traffic rate in kbps. Range is 1-1000000

`BURST` = Normal burst size in kbps. Range is 0-20000

`Exceed-burst-size` = Specify an exceed burst size in (kbps) EBS <1-20000>

`exceed-action drop` = Specify dropping the packet when rates are exceeded

6.19.2 Command Mode

Class mode

6.19.3 Example

```
# configure terminal
(config)# policy-map pmap1
(config-pmap)# class cmap1
(config-pmap-c)# police 48000 8000 exceed-action drop
```

6.19.4 Related Commands

`class, policy map, show policy-map`

6.20 police-aggregate

Use this command to apply an aggregate policer to multiple classes in the same policy map. Use the `no` parameter with this command to delete an aggregate policer from a policy map.

6.20.1 Command Syntax

`(no) police-aggregate NAME`

`NAME` = Aggregate-policer name

6.20.2 Command Mode

Class mode

6.20.3 Usage

Use the `police-aggregate` command to apply the aggregate policer named in the `mls qos aggregate-police` command to multiple classes in the same policy map.

6.20.4 Example

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

```
# configure terminal
(config)# ip-access-list 1 permit 10.1.0.0 0.0.255.255
(config)# ip-access-list 2 permit 11.3.1.1
(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
drop
(config)# class-map cmap1
(config-cmap)# match access-group 1
```

```
(config-cmap)# exit
(config)# class-map map cmap2
(config-cmap)# match access-group 2
(config-cmap)# exit
(config)# policy-map aggflow1
(config-pmap)# class cmap1
(config-pmap-c)# police-aggregate transmit1
(config-pmap-c)# exit
(config-pmap)# class cmap2
(config-pmap-c)# set ip-dscp 56
(config-pmap-c)# police-aggregate transmit1
(config-pmap-c)# exit
(config-pmap)# exit
(config)# interface ge1
(config-if)# service-policy input aggflow1
```

6.20.5 Related Commands

`class, policy map, mls qos aggregate-police`

6.21 policy-map

Use this command to create a policy map. Use the `no` parameter with this command to delete an existing policy map.

6.21.1 Command Syntax

`(no) policy-map NAME`

`NAME` = Name of the policy map

6.21.2 Command Mode

Configure mode

6.21.3 Example

```
# configure terminal
(config)# policy-map pmap1
```

6.21.4 Related Commands

`class, class-map, police, show policy-map`

6.22 service-policy input

Use this command to apply a policy map to the input of an interface. Use the `no` parameter with this command to remove a policy map and interface association.

6.22.1 Command Syntax

`(no) service-policy input INPUT NAME`

`INPUT NAME` = Policy map name

6.22.2 Command Mode

Interface mode

6.22.3 Example

```
# configure terminal
(config)# interface ge1
(config-if)# service-policy input pmap1
```

6.22.4 Related Commands

`policy-map`

6.23 set cos

Use this command to set a CoS value to assign to classified traffic, or enable copying of priority bit (pbit) from the inner VLAN to the outer VLAN, based on policy. Use the `no` parameter with this command to remove a CoS value, or disable pbit copying.

6.23.1 Command Syntax

`(no) set cos COS_VALUE|cos-inner`

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

`cos-inner` = Copy pbit from the inner VLAN to the outer VLAN, based on policy

6.23.2 Command Mode

Class mode

6.23.3 Example

```
# configure terminal
(config)# policy-map pmap1
(config-pmap)# class cmap1
(config-pmap-c)# set cos 2
```

6.23.4 Related Commands

`class, policy-map, set ip-dscp, set ip-precedence`

6.24 set ip-dscp

Use this command to set a DSCP value to assign to classified traffic. Use the `no` parameter with this command to remove a DSCP value.

6.24.1 Command Syntax

`(no) set ip-dscp <0-63>`

6.24.2 Command Mode

Class mode

6.24.3 Example

```
# configure terminal
(config)# policy-map pmap1
(config-pmap)# class cmap1
(config-pmap-c)# set ip-dscp 40
```

6.24.4 Related Commands

`class, policy-map, set cos, set ip-precedence`

6.25 set ip-precedence

Use this command to set an IP-precedence value to assign to classified traffic. Use the no parameter with this command to remove an IP-precedence value.

6.25.1 Command Syntax

```
(no) set ip-precedence <0-7>
```

6.25.2 Command Mode

Class mode

6.25.3 Example

```
# configure terminal
(config)# policy-map pmap1
(config-pmap)# class cmap1
(config-pmap-c)# set ip-precedence 2
```

6.25.4 Related Commands

`class, policy-map, set ip cos, set ip dscp`

6.26 set mpls exp-bit topmost

Use this command to set the MPLS experimental-bit value in the topmost label for a policy map. Use the no parameter with this command to remove this setting from a policy map.

6.26.1 Command Syntax

```
(no) set mpls exp-bit topmost <0-7>
```

`<0-7>` Experimental value

6.26.2 Command Mode

Policy Map Class mode

6.26.3 Usage

Set a new MPLS experimental-bit value in a packet to classify MPLS traffic.

6.26.4 Example

The following example shows configuring a policy map named pmap1 for class map cmap 1, and setting the MPLS experimental-bit value to 7 in a packet.

```
(config)# policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set mpls exp-bit topmost 7
```

6.27 show class-map

Use this command to display the QoS class maps to define the match criteria to classify traffic.

6.27.1 Command Syntax

```
show class-map NAME
```

`NAME` = Name of the class map

6.27.2 Command Mode

Exec mode and Privileged Exec mode

6.27.3 Example

```
# show class-map cmap1
CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
```

6.27.4 Related Commands

`class-map`

6.28 show mls qos aggregator-policer

Use this command to display the aggregate policer configuration.

6.28.1 Command Syntax

```
show mls qos aggregator-policer NAME
```

`NAME` = Name of the aggregate policer

6.28.2 Command Mode

Exec mode and Privileged Exec mode

6.28.3 Example

```
#show mls qos aggregator-policer agp1 AGGREGATOR-POLICER-NAME: agp1
    Police:    Average rate(1 kbps), burst size(1 kilobytes)    Exceed-
action drop
```

6.28.4 Related Commands

```
mls qos aggregate-police
```

6.29 show mls qos interface

Use this command to display queueing and scheduling information for an interface.

6.29.1 Command Syntax

```
show mls qos interface IFNAME
```

`IFNAME` = Interface name

6.29.2 Command Mode

Exec mode and Privileged Exec mode

6.29.3 Example

```
#show mls qos interface ge17
  INPUT-POLICY-MAP-NAME: pmap1
    CLASS-MAP-NAME: cmap1
      Match vlan: 20
  Schedule mode: strict
    The number of egress queue: 8
    Weights (priority): 0(1), 0(2), 0(3), 0(4), 0(5), 0(6), 0(7), 0(7)

#show mls qos interface ge17
  INPUT-POLICY-MAP-NAME: pmap1
    CLASS-MAP-NAME: cmap1
      Match vlan: 20
  Schedule mode: weighted round-robin
    The number of egress queue: 8
    Weights (priority): 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7), 0(7)
```

Schedule mode displays `strict` only when the entire queue weights are 0, otherwise, it displays as `weighted round-robin`.

6.30 show mls qos maps dscp-cos

Use this command to display DSCP-to-CoS mapping information.

6.30.1 Command Syntax

`show mls qos maps dscp-cos UNIT-NAME`

`UNIT-NAME` = Name of the unit

6.30.2 Command Mode

Exec mode and Privileged Exec mode

6.30.3 Example

```
#show mls qos maps dscp-cos base  DSCP-TO-COS-MAP:  base
    d1 :   d2  0   1   2   3   4   5   6   7   8   9
    ------------------------------------------------
     0 :       4   4   4   4   4   4   4   4   1   1
     1 :       1   1   1   1   1   1   2   2   2   2
     2 :       2   2   2   2   3   3   3   3   3   3
     3 :       3   3   4   4   4   4   4   4   4   4
     4 :       5   5   5   5   5   5   5   5   6   6
     5 :       6   6   6   6   6   6   7   7   7   7
     6 :       7   7   7   7
```

6.30.4 Related Commands

`mls qos map dscp-cos`

6.31 show mls qos maps dscp-mutation

Use this command to display DSCP-to-DSCP mutation mapping information.

6.31.1 Command Syntax

`show mls qos maps dscp-mutation UNIT-NAME`

`UNIT-NAME` = Name of the unit

6.31.2 Command Mode

Exec mode and Privileged Exec mode

6.31.3 Example

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

6.31.4 Related Commands

`mls qos map dscp-mutation`

6.32 show policy-map

Use this command to display QoS policy map information.

6.32.1 Command Syntax

`show policy-map NAME`

`NAME` = Name of the policy map

6.32.2 Command Mode

Exec mode and Privileged Exec mode

6.32.3 Example

```
#show policy-map mapa class pmap1
POLICY-MAP-NAME: pmap1
    State: detached

    CLASS-MAP-NAME: cmap1
```

```
      Set IP DSCP: 56
      Match IP DSCP: 7
  POLICY-MAP-NAME: pmap1
    State: detached

    CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
```

6.32.4 Related Commands

`policy-map`

6.33 show qos-access-list

Use this command to display IP and MAC ACLs.

6.33.1 Command Syntax

`show qos-access-list ACCESS-LIST NUMBER|WORD`

`NUMBER` = Access-list number

`<1-99>` = Range for IP standard ACL

`<100-199>` = Range for IP extended ACL

`<1300-1999>` = Expanded range for IP standard ACL

`<2000-2699>` = Expanded range for IP extended ACL

`WORD` = Access-list name

6.33.2 Command Mode

Exec mode and Privileged Exec mode

6.33.3 Example

```
#show qos-access-list 1
  Standard IP-QOS-ACCESS-LIST: 1
    permit 11.11.11.50
```

6.33.4 Related Commands

`ip-access-list, mac-access list`

6.34 wrr-queue bandwidth

Use this command to specify the bandwidth ratios of the transmit queues. Use the no parameter with this command to return to the default bandwidth.

6.34.1 Command Syntax

`wrr-queue bandwidth WRR_WTS`

`(no) wrr-queue bandwidth`

`WRR_WTS` = Weighted Round Robin (WRR) weights for the 8 queues (8 values separated by spaces). Range is 1-65535.

6.34.2 Command Mode

Configure mode

6.34.3 Example

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue bandwidth 100 300 400 200 600 800 700 1000
```

6.34.4 Related Commands

`wrr-queue queue-limit`

6.35 wrr-queue cos-map

Use this command to specify CoS values for a queue. Use the no parameter with this command to return to the default setting.

6.35.1 Command Syntax

`wrr-queue cos-map QUEUE_ID COS_VALUE`

`(no) wrr-queue cos-map`

`QUEUE_ID` = Queue ID. Range is 0-7

`COS_VALUE` = CoS values. Up to 8 values (separated by spaces). Range is 0-7.

6.35.2 Command Mode

Configure mode

6.35.3 Usage

A maximum of 8 CoS values can be used to create the CoS map.

6.35.4 Example

The following example shows mapping CoS values 0 and 1 to queue 1.

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue cos-map 1 0 1
```

6.36 wrr-queue dscp-map

Use this command to map the DSCP values to the Weighted Random Early Detection (WRED) thresholds of an egress queue. Use the no parameter with this command to return to the default setting.

6.36.1 Command Syntax

`wrr-queue dscp-map THRESHOLD_ID DSCP_VALS`

`(no) wrr-queue dscp-map THRESHOLD_ID`

`THRESHOLD_ID` = Queue threshold ID. Range is 1-2.

`DSCP_VALS` = DSCP values mapped to a threshold ID; each value separated by 1 space. Range is 0-63. A maximum of 8 DSCP values can be entered per command.

6.36.2 Command Mode

Configure mode

6.36.3 Example

The following example shows mapping DSCP values 0 to 9 to threshold 1, and DSCP values 10 to 14 to threshold 2.

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue dscp-map 1 0 1 2 3 4 5 6 7
(config-if)# wrr-queue dscp-map 1 8 9
(config-if)# wrr-queue dscp-map 2 10 11 12 13 14
```

6.36.4 Related Commands

`show mls qos interface, wrr-queue cos-map, wrr-queue threshold`

6.37 wrr-queue min-reserve

Use this command to configure the buffer size of the minimum-reserve level for a specific queue. Use the `no` parameter with this command to return to the default setting.

6.37.1 Command Syntax

`wrr-queue min-reserve QUEUE_ID MINRES_LVL`

`(no) wrr-queue min-reserve QUEUE_ID`

`QUEUE_ID` = Queue ID. Range is 0-7.

`MINRES_LVL` = Minimum reserve level. Range is 1-8.

6.37.2 Command Mode

Configure mode

6.37.3 Example

The following example shows assigning a minimum reserve level of 5 to egress queue 1 on fe0.

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue min-reserve 1 5
```

6.37.4 Related Commands

`show mls qos interface`

6.38 wrr-queue queue-limit

Use this command to configure the egress queue size ratios. Use the `no` parameter with this command to return to the default setting.

6.38.1 Command Syntax

`wrr-queue queue-limit QUEUE_WTS`

`(no) wrr-queue queue-limit`

`QUEUE_WTS` = Queue weight ratio for up to 8 queues. Range is 1-100.

6.38.2 Command Mode

Configure mode

6.38.3 Usage

Ratio should total 100 percent.

6.38.4 Example

The following example shows configuring a 75:25 ratio for queues 1 and 2, respectively.

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue queue-limit 75 25
```

6.38.5 Related Commands

`wrr-queue bandwidth`

6.39 wrr-queue random-detect max-threshold

Use this command to configure the WRED drop threshold percentages for an egress queue. Use the `no` parameter with this command to return to the default setting.

6.39.1 Command Syntax

`wrr-queue random-detect max-threshold QUEUE_ID THRESHOLD_WT1 THRESHOLD_WT2`

`(no) wrr-queue random-detect max-threshold QUEUE_ID`

`QUEUE_ID` = Queue ID. Range is 0-7.

`THRESHOLD_WT1` = Low WRED value. Threshold weight in percent. Range is 1-100.

`THRESHOLD_WT2` = High WRED value. Threshold weight in percent. Range is 1-100.

6.39.2 Command Mode

Configure mode

6.39.3 Usage

WRED values are a percentage of queue capacity.

6.39.4 Example

The following example shows configuring threshold percentage weights of 60 and 100 on queue 1.

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue random-detect max-threshold 1 60 100
```

6.39.5 Related Commands

`wrr-queue random-detect max-threshold, wrr-queue queue-limit`

6.40 wrr-queue threshold

Use this command to configure the tail-drop threshold percentages for a queue. Use the no parameter with this command to return to the default setting.

6.40.1 Command Syntax

`wrr-queue threshold QUEUE_ID THRESHOLD_WT1 THRESHOLD_WT2`

`(no) wrr-queue threshold QUEUE_ID`

`QUEUE_ID` = Queue ID. Range is 0-7.

`THRESHOLD_WT1` = Number of weights in percent for threshold 1. Range is 1-100.

`THRESHOLD_WT2` = Number of weights in percent for threshold 2. Range is 1-100.

6.40.2 Command Mode

Configure mode

6.40.3 Example

```
# configure terminal
(config)# interface fe0
(config-if)# wrr-queue threshold 1 60 100
```

6.40.4 Related Commands

`wrr-queue queue-limit`

Debug and Error Commands

7.1 debug nsm

Use this command to specify a set of debug options for NSM events, kernel, and packets.

7.1.1 Command Syntax

`(no) debug nsm`

You can use `all` option along with the `(no) debug nsm` command to specify the set of debug options for NSM events, kernel, and packets.

For example, `no debug nsm all`.

7.1.2 Command Mode

Exec mode, Privileged Exec mode, and Configure mode

7.1.3 Examples

```
# debug nsm
```

7.1.4 Related Commands

`debug nsm kernel, debug nsm events, debug nsm packet`

7.1.5 Validation Commands

`show debugging nsm`

For sample output of the validation commands, refer to *Appendix A, debug nsm on page 257*.

7.2 debug nsm events

Use this command to specify the set of debug options for NSM daemon events.

7.2.1 Command Syntax

`debug nsm events`

7.2.2 Command Mode

Privileged Exec mode and Configure mode

7.2.3 Examples

```
# debug nsm events
```

7.2.4 Related Commands

`debug nsm kernel`

7.2.5 Validation Commands

`show debugging nsm`

For sample output of the validation commands, refer to *Appendix A, debug nsm on page 257*.

7.3 debug nsm kernel

Use this command to specify the debug option-set for the NSM daemon routing manager between the kernel interface.

7.3.1 Command Syntax

`debug nsm kernel`

7.3.2 Command Mode

Privileged Exec mode and Configure mode

7.3.3 Examples

```
# debug nsm kernel
```

7.3.4 Validation Commands

`show debugging nsm`

For sample output of the validation commands, refer to *Appendix A, debug nsm on page 257*.

7.4 debug nsm packet

Use this command to specify the debug option-set for the nsm packet.

7.4.1 Command Syntax

`debug nsm packet (recv|send)(detail)`

`recv` = Specifies the debug option-set for receive packet

`send` = Specifies the debug option-set for send packet

`detail` = Sets the debug option set to detailed information

7.4.2 Command Mode

Privileged Exec mode and Configure mode

7.4.3 Examples

```
# debug nsm packet
# debug nsm packet recv detail
```

7.4.4 Validation Commands

`show debugging nsm`

For sample output of the validation commands, refer to *Appendix A, debug nsm on page 257*.

7.5 error-threshold enable

Use this command to enable/disable the port error notifications to the SRS-API.

7.5.1 Command Syntax

`error-threshold (enable interval <interval-value> | disable)`

`interval-value = 10 - 10800 seconds`

By default this is disabled.

7.5.2 Command mode

Configure mode

7.5.3 Usage

This command enables error notifications and sets a timer for the configured interval. Error notifications are sent by checking the error count at configured interval seconds.

7.5.4 Examples

```
#configure terminal
(config)# error-threshold enable interval 100
```

7.5.5 Validation Commands

`show running-config`

For sample output of the validation commands, refer to Appendix A, *error-threshold enable on page 259*.

7.5.6 Related commands

`error-threshold`

7.6 error-threshold (crc|alignment |badsymbol)

Use this command to configure thresholds for various types of errors.

7.6.1 Command Syntax

```
error-threshold (crc|alignment|badsymbol) <threshold-range> (shutdown | )
threshold-range = <1-4294967295>
(no)  error-threshold (crc|alignment|badsymbol)
```

7.6.2 Command mode

Interface mode

7.6.3 Usage

Asynchronous events are sent when the configured threshold is hit in the interval for a specific error on a particular port. Asynchronous events are sent through SRS-API only if the error-threshold is enabled through error-threshold enable command.

"Shutdown" is optional and when "shutdown" option is specified, SRS will shutdown the port apart from sending asynchronous events.

7.6.4 Examples

```
#configure terminal
(config-if)# error-threshold crc 200 shutdown
```

7.6.5 Validation

```
show running-config, show error-threshold
```

7.6.6 Related commands

```
error-threshold enable
```

7.7 no debug nsm events

Use this command to disable the debugging options for NSM daemon events.

7.7.1 Command Syntax

```
no debug nsm events
```

7.7.2 Command Mode

Privileged Exec mode and Configure mode

7.7.3 Examples

```
# no debug nsm events
```

7.7.4 Equivalent Commands

```
undebug nsm events
```

7.8 no debug nsm kernel

Use this command to disable the debugging option for the NSM daemon routing manager between the kernel interface.

7.8.1 Command Syntax

```
no debug nsm kernel
```

7.8.2 Command Mode

Privileged Exec mode and Configure mode

7.8.3 Examples

```
# no debug nsm kernel
```

7.8.4 Equivalent Commands

```
no debug nsm kernel
```

7.9 no debug nsm packet

Use this command to disable the debugging option for the NSM packet.

7.9.1 Command Syntax

`no debug nsm packet (recv|send)(detail)`

`recv` = Disable the debugging option for receive packet

`send` = Disable the debugging option for send packet

`detail` = Disable the debugging option for detailed information

7.9.2 Command Mode

Privileged Exec mode and Configure mode

7.9.3 Examples

```
# no debug nsm packet
# no debug nsm packet recv detail
```

7.9.4 Validation Commands

`show debugging nsm`

For sample output of the validation commands, refer to Appendix A, *no debug nsm packet on page 262*.

7.9.5 Equivalent Commands

`no debug nsm packet`

7.10 show debugging nsm

Use this command to display debugging information for the SRstackware routing manager.

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, SRstackware CLI Environment on page 41*.

7.10.1 Command Syntax

`show debugging nsm`

7.10.2 Command Mode

Exec mode and Privileged Exec mode

7.10.3 Usage

The following is a sample output of the `show debugging nsm` command displaying the NSM debugging status.

```
# show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
```

7.10.4 Examples

```
# show debugging nsm
```

7.11 show error-threshold

Use this command to display port (s) errors threshold.

7.11.1 Command Syntax

```
show error-threshold (interface IFNAME | )
```

7.11.2 Command mode

Exec mode and Privileged Exec mode

7.11.3 Usage

This shows the configured errors, thresholds, and shutdown action if specified on all the configured interface(s). The following is the sample output of this command.

```
#show error-threshold interface ge45
Interface ge45
 error-threshold crc 10
 error-threshold alignment 20 shutdown
 error-threshold badsymbol 30
```

7.11.4 Examples

```
#show error-threshold interface ge45
#show error-threshold
```

7.12 undebug nsm

Use this command to disable all NSM debugging.

7.12.1 Command Syntax

undebug nsm

You can use `all` option along with the `undebug nsm` command to disable all NSM debugging.

For example, `undebug nsm all`.

7.12.2 Command Mode

Privileged Exec mode

7.12.3 Examples

```
# undebug nsm
```

7.13 undebug nsm events

Use this command to disable the debugging options for NSM daemon events.

7.13.1 Command Syntax

undebug nsm events

7.13.2 Command Mode

Privileged Exec mode

7.13.3 Examples

```
# undebug nsm events
```

7.14 undebug nsm kernel

Use this command to disable the debugging option for the NSM daemon routing manager between the kernel interface.

7.14.1 Command Syntax

```
undebug nsm kernel
```

7.14.2 Command Mode

Privileged Exec mode

7.14.3 Examples

```
# undebug nsm kernel
```

7.15 undebug nsm packet

Use this command to disable the debugging option for the nsm packet.

7.15.1 Command Syntax

```
undebug nsm packet (recv|send)(detail)
```

`recv` = Disable the debugging option for receive packet

`send` = Disable the debugging option for send packet

`detail` = Disable the debugging option for detailed information

7.15.2 Command Mode

Privileged Exec mode

7.15.3 Examples

```
# undebug nsm packet
# undebug nsm packet recv detail
```

7.15.4 Validation Commands

```
show debugging nsm
```

For sample output of the validation commands, refer Appendix A, *undebug nsm packet on page 262*.

Validation Commands Sample Output

A.1 Overview

This chapter provides the sample outputs of the validation commands.

A.2 access-lists

This command is available only if LAYER3SRS is licensed.

A.2.1 show ip access-list

```
atca-blade-6#show ip access-list
ZebOS IP access list mylist
 deny   10.10.0.72/24 exact-match
ZebOS IP access list mylist1
 permit any
```

A.2.2 show running-config

```
blade-SLOT1#show running-config
----
----
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
```

```
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface xe38
 description Fabric Front Panel QSFP 40G (ETH2)
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
!
```

```
 interface vlan1.93
  no shutdown
 !
 interface vlan2.1
  shutdown
 !
 interface vlan2.11
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.11.1/24
  no shutdown
 !
 interface vlan2.12
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.12.1/24
  no shutdown
 !
 interface vlan2.91
  no shutdown
 !
access-list mylist deny 10.10.0.72/24 exact-match
access-list mylist1 permit any
!
line con 0
 login
line vty 0 4
 login
!
```

A.2.3 show ipv6 access-list

```
atca-blade-6#show ipv6 access-list
ZebOS IPv6 access list mylist
    deny   3ffe:506::/32 exact-match
    permit any
atca-blade#
```

A.3 access-list extended

This command is available only if LAYER3SRS is licensed.

A.3.1 show ip access-list

```
atca-blade-6#show ip access-list
Extended IP access list 134
    deny ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255
Extended IP access list 2345
    permit ip host 10.10.2.76 host 20.20.2.70
```

A.3.2 show running-config

```
blade-SLOT1#show running-config
----
----
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
```

```
 shutdown
!
interface xe38
 description Fabric Front Panel QSFP 40G (ETH2)
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
```

```
 shutdown
!
interface vlan2.11
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.11.1/24
 no shutdown
!
interface vlan2.12
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.12.1/24
 no shutdown
!
interface vlan2.91
 no shutdown
!
access-list 134 deny ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255
access-list 2345 permit ip host 10.10.2.76 host 20.20.2.70
!
line con 0
login
line vty 0 4
login
!
```

A.3.3 show ipv6 access-list

```
atca-blade-6#show ipv6 access-list
ZebOS IPv6 access list mylist
    deny   3ffe:506::/32 exact-match
    permit any
atca-#
```

A.4 access-list standard

This command is available only if LAYER3SRS is licensed.

A.4.1 show running-config

```
blade-SLOT1#show running-config
----
----
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe38
  description Fabric Front Panel QSFP 40G (ETH2)
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
```

```
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
 shutdown
!
interface vlan2.11
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.11.1/24
 no shutdown
!
```

```
 interface vlan2.12
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.12.1/24
  no shutdown
 !
 interface vlan2.91
  no shutdown
 !
access-list 67 deny 1.1.1.0 0.0.0.255
access-list 1332 permit any
!
line con 0
login
line vty 0 4
login
!
```

A.4.2 show ipv6 access-list

```
atca-blade-6#show ipv6 access-list
ZebOS IPv6 access list mylist
    deny   3ffe:506::/32 exact-match
    permit any
atca-blade#
```

A.5 bandwidth

A.5.1 show interface ge21

```
atca-blade-6#show interface ge21
Interface ge21
Hardware is Ethernet
Current HW addr: 00c8.aaa7.0017
Physical:00c8.aaa7.0017
Description: Base RTM SFP 1G Uplink 1 (ETH8)
```

```
index 5021 metric 1 mtu 1500 duplex-full arp ageing timeout 0
<UP,BROADCAST,MULTICAST>
VRF Binding: Not bound
Bandwidth 1g
VRRP Master of :  VRRP is not configured on this interface.
input packets 00, bytes 00, dropped 00, multicast packets 00
output packets 00, bytes 00, multicast packets 00 broadcast packets 00
atca-blade-6#
```

A.5.2 show running-config

```
blade-SLOT1#show running-config
----
interface xe3
description Base Front Panel SFP+ 10G Link 1(ETH3)
duplex full
bandwidth 1g
bridge-group 1 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 94
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 94 egress-tagged disable
 no shutdown
!
---
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
```

```
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface xe38
 description Fabric Front Panel QSFP 40G (ETH2)
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
```

```
 !
 interface vlan1.93
  no shutdown
 !
 interface vlan2.1
  shutdown
 !
 interface vlan2.11
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.11.1/24
  no shutdown
 !
 interface vlan2.12
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.12.1/24
  no shutdown
 !
 interface vlan2.91
  no shutdown
 !
bridge-group 1
vlan classifier activate 1 vlan 5
 no shutdown
```

A.6 duplex

A.6.1 show interface ge21

```
atca-blade-6#show interface ge21
Interface ge21
Hardware is Ethernet
Current HW addr: 00c8.aaa7.0017
 Physical:00c8.aaa7.0017
```

```
 Description: Base RTM SFP 1G Uplink 1 (ETH8)
 index 5021 metric 1 mtu 1500 duplex-full arp ageing timeout 0
 <UP,BROADCAST,MULTICAST>
 VRF Binding: Not bound
 Bandwidth 1g
 VRRP Master of :  VRRP is not configured on this interface.
input packets 00, bytes 00, dropped 00, multicast packets 00
output packets 00, bytes 00, multicast packets 00 broadcast packets 00
atca-blade-6#
```

A.6.2 show running-config interface

```
atca-blade-6#show running-config interface ge21
!
interface ge21
description Base RTM SFP 1G Uplink 1 (ETH8)
duplex full
bandwidth 1g
bridge-group 1
vlan classifier activate 1 vlan 5
no shutdown
```

A.7 hostname

A.7.1 show running-config

```
atca-blade-6#show running-config
(config)# hostname IPI
```

After command:

```
IPI(config)#
```

A.8 ipv6 access-list

This command is available only if LAYER3SRS is licensed.

A.8.1 show ipv6 access-list

```
atca-blade-6#show ipv6 access-list
ZebOS IPv6 access list mylist
 deny   3ffe:506::/32 exact-match
 permit any
```

A.8.2 show running-config

```
blade-SLOT1#show running-config
----
----
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
```

```
!
interface xe38
 description Fabric Front Panel QSFP 40G (ETH2)
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
 shutdown
```

```
 !
 interface vlan2.11
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.11.1/24
  no shutdown
 !
 interface vlan2.12
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.12.1/24
  no shutdown
 !
 interface vlan2.91
  no shutdown
 !
ipv6 access-list mylist deny 3ffe:506::/32 exact-match
ipv6 access-list mylist permit any
!
route-map mymap1 permit 10
!
line con 0
 login
line vty 0 5
 login
!
```

A.9 line vty

A.9.1 show running-config

```
atca-blade-6(config-line)#show running-config | include vty
line vty 0 5
```

A.10 log file

A.10.1 show running-config

```
blade-SLOT1#show running-config
----
!
log file /usr/local/sbin/bgpd.log
!
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe38
  description Fabric Front Panel QSFP 40G (ETH2)
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
```

```
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
 shutdown
!
interface vlan2.11
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.11.1/24
 no shutdown
!
interface vlan2.12
 no switchport
```

```
 arp-ageing-timeout 3000
 ip address 192.168.12.1/24
 no shutdown
!
interface vlan2.91
 no shutdown
!
line con 0
 login
line vty 0 4
 login
!
end
```

A.11 log record-priority

A.11.1 show running-config

```
blade-SLOT1#show running-config
----
!
log file /usr/local/sbin/bgpd.log
log trap informational
log record-priority
!
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
```

```
interface xe37
 description Fabric Front Panel QSFP 10G (ETH1) - Port 4
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface xe38
 description Fabric Front Panel QSFP 40G (ETH2)
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
```

```
 ip address 192.168.24.1/24
 no shutdown
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
 shutdown
!
interface vlan2.11
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.11.1/24
 no shutdown
!
interface vlan2.12
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.12.1/24
 no shutdown
!
interface vlan2.91
 no shutdown
!
line con 0
 login
line vty 0 4
 login
!
end
```

A.12 log trap

A.12.1 show running-config

```
blade-SLOT1#show running-config
----
!
log file /usr/local/sbin/bgpd.log
log trap informational
!
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe38
  description Fabric Front Panel QSFP 40G (ETH2)
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
```

```
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
 shutdown
!
interface vlan2.11
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.11.1/24
 no shutdown
!
interface vlan2.12
```

```
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.12.1/24
 no shutdown
!
interface vlan2.91
 no shutdown
!
line con 0
 login
line vty 0 4
 login
!
end
```

A.13 rule match-list

A.13.1 show rule match-list

```
atca-blade-6#show rule match-list
match-list 2 unit base
  Actions:
    modify-dscp 30
    modify-vlanid 10
match-list 4 unit base
  Actions:
    modify-dscp 30
    modify-vlanid 10
atca-blade-6#
```

A.13.2 show running-config

```
blade-SLOT1#show running-config
----
----
----
```

```
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe38
  description Fabric Front Panel QSFP 40G (ETH2)
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface vlan1.1
  no shutdown
 !
 interface vlan1.21
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.21.1/24
  no shutdown
 !
```

```
 interface vlan1.22
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.22.1/24
  no shutdown
 !
 interface vlan1.24
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.24.1/24
  no shutdown
 !
 interface vlan1.93
  no shutdown
 !
 interface vlan2.1
  shutdown
 !
 interface vlan2.11
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.11.1/24
  no shutdown
 !
 interface vlan2.12
  no switchport
  arp-ageing-timeout 3000
  ip address 192.168.12.1/24
  no shutdown
 !
 interface vlan2.91
  no shutdown
 !
match-list 2 base
match-list 3 base
match-list 4 base
```

```
match-list 5 base
!
rule match-list 2 action modify-dscp 30 modify-vlanid 10
rule match-list 3 action modify-dscp 30 modify-vlanid 10
rule match-list 4 action modify-dscp 30 modify-vlanid 10
rule match-list 5 action modify-dscp 30 modify-vlanid 10
!
 line con 0
  login
 line vty 0 4
  login
 !
 end
```

A.14 debug nsm

A.14.1 show debugging nsm

```
atca-blade-6#show debugging nsm

NSM debugging status:
  NSM event debugging is on
  NSM packet detail debugging is on
  NSM kernel debugging is on
  NSM HA all debugging is on

atca-blade-6#
```

A.15 debug nsm events

A.15.1 show debugging nsm

```
atca-blade-6#show debugging nsm

NSM debugging status:
  NSM event debugging is on
  NSM packet detail debugging is on
  NSM kernel debugging is on
  NSM HA all debugging is on

atca-blade-6#
```

A.16 debug nsm kernel

A.16.1 show debugging nsm

```
atca-blade-6#show debugging nsm

NSM debugging status:
  NSM event debugging is on
  NSM packet detail debugging is on
  NSM kernel debugging is on
  NSM HA all debugging is on

atca-blade-6#
```

A.17 debug nsm packet

A.17.1 show debugging nsm

```
atca-blade-6#show debugging nsm

NSM debugging status:
  NSM event debugging is on
  NSM packet detail debugging is on
  NSM kernel debugging is on
  NSM HA all debugging is on

atca-blade-6#
```

A.18 error-threshold enable

A.18.1 show running-config

```
blade-SLOT1#show running-config
----
!
error-threshold enable interval 100
!
----
interface xe36
  description Fabric Front Panel QSFP 10G (ETH1) - Port 3
  bridge-group 2 spanning-tree disable
  switchport mode hybrid
  switchport hybrid vlan 91
  switchport mode hybrid acceptable-frame-type all
  switchport hybrid allowed vlan add 91 egress-tagged disable
  shutdown
 !
 interface xe37
  description Fabric Front Panel QSFP 10G (ETH1) - Port 4
```

```
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface xe38
 description Fabric Front Panel QSFP 40G (ETH2)
 bridge-group 2 spanning-tree disable
 switchport mode hybrid
 switchport hybrid vlan 91
 switchport mode hybrid acceptable-frame-type all
 switchport hybrid allowed vlan add 91 egress-tagged disable
 shutdown
!
interface vlan1.1
 no shutdown
!
interface vlan1.21
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.21.1/24
 no shutdown
!
interface vlan1.22
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.22.1/24
 no shutdown
!
interface vlan1.24
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.24.1/24
 no shutdown
```

```
!
interface vlan1.93
 no shutdown
!
interface vlan2.1
 shutdown
!
interface vlan2.11
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.11.1/24
 no shutdown
!
interface vlan2.12
 no switchport
 arp-ageing-timeout 3000
 ip address 192.168.12.1/24
 no shutdown
!
interface vlan2.91
 no shutdown
!
line con 0
 login
line vty 0 4
 login
!
end
```

A.19 no debug nsm packet

A.19.1 show debugging nsm

```
atca-blade-6#show debugging nsm

NSM debugging status:
  NSM event debugging is on
  NSM kernel debugging is on
  NSM HA all debugging is on

atca-blade-6#
```

A.20 undebug nsm packet

A.20.1 show debugging nsm

```
atca-blade-6#show debugging nsm

NSM debugging status:
NSM event debugging is on
 NSM kernel debugging is on
 NSM HA all debugging is on

atca-blade-6#
```

Rx/Tx Drop Counters

NOTICE

Below Drop-counters are independent of each other. If one or more drop-counters are sharing a common trigger-reason, and a packet is dropped due to that particular trigger-reason, the corresponding drop-counters will be incremented independently. As different registers will be chosen for representing a trigger-reason across different Broadcom chipsets, the mapping between Drop-counters to trigger-reasons may vary from Base to Fabric chipsets.

NOTICE

`IfInDiscards` accounts for most significant trigger-reasons to drop a packet.

Input dropped count in `show interface` CLI output reflects the value of `IfInDiscards` counter. The rest of the Rx Drop-counters are basically meant for debug purpose.

On ATCA-F140 Fabric chipset, overflow or congestion drops at port ingress will be explicitly accounted by IfInDiscards.

NOTICE

The below reasons cause `Forwarding Port bitmap to Zero`:

- VLAN check failed
- MTU check failed
- Field processor Drop bit is set
- MPLS packet sequence check failed
- Remote is in HOL state
- **`Source_modid`** is equal to **`My_modid`** in HiGig header
- Unknown header type in HiGig2 header format
- Unknown HiGig OPCODE

B.1 Rx Drop Counters

Following table maps the Rx Drop counters (CLI/SNMP) with the corresponding trigger reasons.

Table B-1 Rx Drop Counters with Corresponding Trigger Reasons

CLI Drop Counter	SNMP Object	Trigger Reason
IfInDiscards	srsReceiveDropSet0	• Packets dropped when ingress port is not in forwarding state. • Receive IPv4 L3 discard packets. • Receive IPv6 L3 discard packet. • A receive policy to discard packets with a particular Source/Destination address or to support Storm Control. • Packets dropped by FP, i.e. Field Processor. • Discard at Port Ingress due to Cell Buffer Pool memory is full. • Forwarding Port bitmap is Zero. • Receive VLAN drop cases.
MCInDiscards	srsReceiveDropSet2	The number of Multicast (L2+L3) packets that are dropped.
FP|PolicyDiscards	srsReceiveDropSet3	• A receive policy to discard packets with a particular Source/Destination address or to support Storm Control. • Packets dropped by FP, i.e. Field Processor.
VLANInDiscards	srsReceiveDropSet4	The number of Received VLAN packets that are dropped.
FwdPbmpZeroDrop|Tunnel|ParityDiscards	srsReceiveDropSet5	• Forwarding Port bitmap is Zero. • Packets trapped to CPU due to egress L3 MTU violation. • Parity error packets. • Receive tunnel error packets.
STPBlock|CellBufferPoolFullDiscards	srsReceiveDropSet6	• Discard at Port Ingress due to Cell Buffer Pool memory is full. • Packets dropped when ingress port is not in forward state.

Table B-1 Rx Drop Counters with Corresponding Trigger Reasons

CLI Drop Counter	SNMP Object	Trigger Reason
L3Discards	srsReceiveDropSet7	• Receive IPv4 L3 discard packets. • Receive IPv4 header error packets. • Receive IPv6 L3 discard packet. • Receive IPv6 header error packets.
HG|DOS|LAG|MCErrorDiscards	srsReceiveDropSet8	• DOS L3 header error packets. • DOS L4 header error packets. • DOS ICMP error packets. • DOS fragment error packets. • HiGig Header error packets. • Multicast Index error packets. • LAG failover loopback packets. • LAG backup port down. • Unknown HiGig header type packet.

B.2 Tx Drop Counters

Following table maps the Tx Drop counters (CLI/SNMP) with the corresponding Trigger reasons.

Table B-2 Tx Drop Counters with Corresponding Trigger Reasons

CLI Drop Counter	SNMP Object	Reason for Triggering
IfOutDiscards	srsTransmitDropSet3	Packets dropped due to any condition.
MCOutDiscards	srsTransmitDropSet5	• Transmit IPv4 IPMC Aged and Drop packets. • Transmit IPv6 IPMC Aged and Drop packets.
Ipv6IfStatsOutDiscards	srsTransmitDropSet1	• Transmit IPv6 IPMC Aged and Drop packets. • Transmit IPv6 L3 UC Aged and Drop packets.
STPBlockDiscards	srsTransmitDropSet6	Packets dropped due to STP State not in forwarding state.
L2MC|VXLTMissDiscards	srsTransmitDropSet7	• L2 MC packet drop counter. • Packets dropped due to miss in VXLT table counter.

Table B-2 Tx Drop Counters with Corresponding Trigger Reasons

CLI Drop Counter	SNMP Object	Reason for Triggering
VLANOutDiscards	srsTransmitDropSet8	• Transmit Tunnel error packets. • Packets dropped when CFI set & Pkt is untagged or L3 switched for IPMC. • Packets dropped due to invalid VLAN counter.
AgedDiscards	srsTransmitDropSet9	• Packets dropped due to TTL threshold counter. • Packets dropped due to packet aged counter. • Transmit IPv4 L3 UC Aged and Drop packets.
HG|L2MTU|ParityDiscards	srsTransmitDropSet10	• Unknown HiGig2 Drop. • Unknown HiGig drop. • L2 MTU fail drop. • Parity Error drop.
IPLen|SIP|LargeDiscards	srsTransmitDropSet11	• IP Length check fail drop. • SIP Link Local Drop flag. • MODID greater than 31 drop counter. • Byte additions too large drop counter.

SRS Fixed MAC Address Implementation

C.1 Overview

The MAC addresses of the SRStackware® interfaces are randomly generated based on seed. Previously, the current time-spec is used as a seed. Since the time-spec changes for each boot, SRStackware ports MAC addresses change for every boot. This implementation is changed; instead of current time-spec that varies for each boot, blade's first MAC address is used as a seed, which is unique for each blade. With this implementation, SRstackware ports' MAC addresses do not change for every reboot, which have multiple advantages. Along with this, to deduce the MAC address of an Inter-Vlan interface from a payload blade or AMC, one x86 application (srs_get_mac_x86) is provided with SRstackware RPM, which is installed at `/opt/srstackware/bin` on the ATCA-F140 blade. User need to copy this application from the location to payload/AMC blade.

Following is the syntax to use the application:

Copy the `srs_get_mac_x86 from /opt/srstackware/bin` to any x86 machine and run `srs_get_mac_x86 <MAC address> <Bridge ID> <Vlan ID>` command.

`MAC address =` MAC address of first ATCA-F140 Ethernet interface without any delimiter.

`BRIDGE-ID =` Bridge number

`VLAN-ID =` VLAN ID of the Inter-Vlan interface

For example, following is the command to get VLAN1.24 MAC address:
`./srs_get_mac_x86 EC9ECD041278 1 24`

Output:

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

Generated MAC address for Bridge ID:1 and Vlan ID:24

0268.e6ff.1115

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

Related Documentation

D.1 Penguin Solutions Documentation

Technical documentation can be found by using the Documentation Search at *https://www.penguinsolutions.com/edge/support/* or you can obtain electronic copies of Penguin Solutions documentation by contacting your local sales representative.

Table D-1 Penguin Solutions Documentation

Document Title	Document 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 Layer 2 Command Reference	6806800N88
SRstackware Intelligent Network Software Layer 3 Command Reference	6806800N93
SRstackware Intelligent Network Software Protocol Demo Guide	6806800N07
SRstackware FAQ	6806800N91

Related Documentation

PENGUIN™
SOLUTIONS