ES 500 Switch Router Command Line Interface Reference

Release 1.0

36-064-01 Rev. 0A

River STONE NETWORKS™

COPYRIGHT NOTICES

© 2002 by Riverstone Networks, Inc. All rights reserved.

Riverstone Networks, Inc.
5200 Great America Parkway
Santa Clara, CA 95054

Printed in the United States of America

This product includes software developed by the University of California, Berkeley, and its contributors.

© 1979 – 1994 by The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley, and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Changes

Riverstone Networks, Inc., and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Riverstone Networks, Inc., to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

Disclaimer

IN NO EVENT SHALL RIVERSTONE NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF RIVERSTONE NETWORKS HAS BEEN ADVISED, KNOWN, OR SHOULD HAVE KNOWN, OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks

Riverstone Networks, Riverstone, RS, and IA are trademarks of Riverstone Networks, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

TABLE OF CONTENTS

LIST OF TABLES

1 PREFACE

This manual provides Command Line Interface (CLI) reference information for commands in the device Switch Router. For product information not available in this manual, see the manuals listed in paragraph "*1.2 Related Documentation*".

1.1 USING THIS GUIDE

The CLI commands and command types are organized alphabetically in this manual. To locate information about a command, go to the chapter for the command. For example, to find information about the "interface add" command, go to the interface Commands chapter, then locate the interface "add command" description within that chapter.

1.2 RELATED DOCUMENTATION

The documentation set includes the following items. Refer to these other documents to learn more about the product.

Table 1-1 Related Documentation

Guide	Contents
Riverstone Networks ES 500 Switch Router Getting Started Guide	Installing and setting up the device
Riverstone Networks ES 500 Switch Router User Guide	How to use CLI (Command Line Interface) commands to configure and manage the device
Riverstone Networks ES 500 Switch Router Message Reference Manual	SYSLOG messages and SNMP traps

2 GETTING STARTED

The CLI is a network management application operated through an ASCII terminal or via Telnet.

Before starting to work with the CLI, the device must be correctly configured (see *Riverstone Networks ES 500 Switch Router Getting Started Guide*), connected and fully functional. The device configuration determines what CLI commands are available and what parameters are active. The required network topology must be prepared with all network information available including IP addresses, VLAN requirements, feature configuration requirements, etc. All passwords and other related permissions must be detailed and available.

The Graphic User Interface (GUI) is terminal based. The prompts display the current command mode the GUI is in.

2.1 INTERFACE COMMANDS

The GUI provides different accesses to enter different commands. After booting up the device, the default command prompt is ">". From this prompt there are the following commands:

Note The system supports code completion. If a command is being entered, the system recognizes what the command is and completes the command.

The available options can be displayed at any time by entering the character "?" and pressing "Enter". The following example displays the command modes.

```
>
>?
Unknown parameter
May be one from the following list:

help      mcli      rs
```

2.1.1 Help

The online help is available under all modes and provides help for the commands in the particular mode.

Note All help is context-sensitive.

To request help enter the character "?" and press "Enter", or if in the middle of entering a command, just press "Enter". All the information or parameter options are displayed. There are different kinds of help information displayed:

- Brief—Displays the command format. Generally shown after a syntax error.
- Command Description— Displays the command description. Generally shown when using "?" within the command name.
- Parameter Description— Displays the command format and description of its parameters. Generally shown when using "?" within the command parameters.

When editing there are defined editing aids to assist in editing. The following table describes the shortcuts.

Table 2-1 Editing Shortcut

Shortcut	Description
CTRL+a	Move to the beginning of a line.
CTRL+e	Move to the end of a line.
CTRL+h	Delete the character to the left of the cursor.
CTRL+j	Carriage return (executes a command).
CTRL+m	Carriage return (executes command).
CTRL+u	Delete the entered line.
CTRL+z	If in a mode, exit back to the next top level. If in the enable mode, exit back to the user mode. If in the configure mode, exit back to the enable mode.
Tab	Completes the command keyword. If the word is not a keyword, a space character is inserted.
Delete	Delete the character to the left of the cursor.
Esc	Stops scrolling screen.
Caps Lock	Functional as standard Caps Lock.
Shift Lock	Functional as standard Shift Lock.

2.1.2 rs

The “rs” command mode is the primary interface to all the CLI commands.

To enter rs commands:

1. At the“>” prompt enter “rs” and press “Enter”. The prompt changes from “>” to “rs>”.

The available commands are as follows:

- Enable—This is used to configure CLI and to display information.
- Help—Provide help (as described above)
- l2-tables—This is to configure and display Layer 2 information.
- System—This is to configure and display “system” commands and configurations.

Enable

The “enable” command mode is the main interface to all the CLI commands.

To enter rs commands:

1. At the “rs>”prompt enter “enable” and press “Enter”. The prompt changes from “rs>” to “rs#”.

From this prompt, CLI commands can be configured or displayed.

2.2 CLI PARAMETER TYPES

The following table describes all the parameter types used with the CLI.

Table 2-2 Parameter Types

Data Type	Description	Example
conditional	A numerical conditional expression. Special symbols are used to describe a numerical condition: > (greater than), < (less than) and != (not equal to).	<1024 or >2048 or !=4096
hexadecimal	A hexadecimal number.	a7 or 0xa7
hostname	IP host Hostname.	gauguin or john-pc
hostname/IP	Hostname or IP address.	nagasaki or 10.43.1.4
keyword	A keyword described in the list of acceptable keywords in the online help.	on or off
interface name or IP address	Name of an interface or its IP address.	int1 or 10.1.4.33
interface name list	A list of one or more interface names delimited by commas.	int1 or int1, int2, int3
IP address	An IP address in the format x.x.x.x. Some commands may explicitly require a Unicast or Multicast address.	10.1.2.3
IP address/mask	A pair of IP address and mask values. Depending on the command, the mask can be a network mask or filtering mask. The mask can be described using the traditional IP address syntax (255.0.0.0) or a CIDR syntax (/8).	10.1.4.0/255.255.255.0 or 10.1.4.0/24
MAC address	A MAC address specified in the following form: xx:xx:xx:xx:xx:xx.	08:00:50:1a:2b:c3
number	An integer number.	100
numerical range	A number or a range of numbers.	5 or 7-10
port	A single port.	et.1.4, gi.2.1, hs.3.1.100, or se.4.2.200
port list	A list of one or more ports. To specify a range of ports, describe the range in parenthesis. Non-consecutive ports can be specified by using commas to separate them. The wildcard character (*) can also be used to specify all ports.	et.1.(3-8) or et.1.(1,3,5), hs.(1-2).1.100, or se.4.(1-3).200, gi.2.*
string	A character string. To include spaces in a string, specify the entire string in double quotes (“).	abc or “abc def”
URL	A Uniform Resource Locator. The type of URL depends on the command where the URL is used. Currently, two URLs are supported: TFTP: *tftp://host/pathname* RCP: *rcp://username@host/pathname*	tftp://10.1.4.5/test/abc.txt rcp://dave@rtr/test/abc.txt

2.3 <*PORTS LIST*> SYNTAX

The <*port-lis*t> parameter is a comma-separated list of ports to be configured. Wildcard or range sequences can be used as the last field of a port name.

Note Where appropriate, the keyword **`all-ports`** may also be used, if a command is to be applied to all the relevant ports.

The syntax for each <*port-lis*t> element is:

<port-type><port>

<port-type>

The interface type being configured can be one of the types shown in Table 2-3.

Table 2-3 Port Types

Port Types	Description
`et`	An Ethernet interface.
`gi`	A Gigabit Ethernet interface.

<port>

The configured port number. The device port types are shown in Table 2-4.

Table 2-4 Device Port Types

Port Types	Description
Ethernet	1 to 24
Gigabit Ethernet	1 to 2

A range of ports can be specified for example 1-4.

3 ACL COMMANDS

The **acl** commands are to create ACLs (Access Control Lists) and apply them to IP interfaces. An ACL permits or denies switching of packets based on criteria such as the packet source address and destination address, TCP or UDP port number, and so on. An ACL can be specified to affect incoming traffic or outgoing traffic.

3.1 COMMAND SUMMARY

The following table lists the **acl** commands. The sections following the table describe the command syntax for each command.

acl *<name>* apply interface *<InterfaceName>* input | output
acl *<name>* apply port *<port list>* input | output
acl *<name>* permit|deny icmp *<SrcAddr/Mask>* *<DstAddr/Mask>*
acl *<name>* permit|deny igmp *<SrcAddr/Mask>* *<DstIP/mask>*
acl <name> permit|deny ip <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
acl *<name>* permit|deny ip-protocol <proto-num> *<SrcAddr/Mask>* *<DstAddr/Mask>* *<tos>* *<tos-mask>*
acl *<name>* permit|deny tcp *<SrcAddr/Mask>* *<DstAddr/Mask>* *<SrcPort>* *<DstPort>* *<tos>* *<tos-mask>*
acl *<name>* permit|deny udp *<SrcAddr/Mask>* *<DstAddr/Mask>* *<SrcPort>* *<DstPort>* *<tos>* *<tos-mask>*
acl show [aclname *<string>*|all]

acl apply interface

Mode

Configure

Format

```
acl <name> apply interface <InterfaceName> input | output
```

Description

The **`acl apply interface`** command creates rules in the device to filter packets. The device filters IP routed packets on an ingress or/and egress ports defined by IP interface with name defined by the ***`InterfaceName`*** parameter. The filtering direction is defined by keywords “input or/and output”. If an interface is defined on a VLAN, then the ingress or/and egress ports defined by this VLAN must be set.

Filters for this command works as for “acl apply port” command on a “First match” basis.

The following table describes the command parameters.

Parameter	Value	Meaning
`acl`	*`<name>`*	ACL name. Use a character or number string up to 15 characters long.
`apply interface`	*`<InterfaceName>`*	Defines interface where packets are filtered.
	`input	output`	Defines which packets are filtered by the direction the packets are flowing.

Restrictions

None

acl apply port

Mode

Configure

Format

```
acl <name> apply port <port list> input | output
```

Description

The **acl apply port** command creates rules in the device to filter packets according to IP flow specifications defined by the command **acl permit|deny**. The device filters l2 switched or IP routed packets on an ingress or/and egress ports defined by the **port list** parameter. The filtering direction is defined by keywords “input or/and output”.

The following table describes the command parameters.

Parameter	Value	Meaning
acl	*<name>*	ACL name. Use a string of characters or a number.
apply port	*<port list>*	Defines ports where packets are filtered .
	input | output	Defines which packets are filtered by the direction the packets are flowing.

Restrictions

None

acl permit|deny icmp

Mode

Configure

Format

```
acl <name> permit|deny icmp <SrcAddr/Mask> <DstAddr/Mask> <tos>
```

Description

The **`acl permit icmp`** and **`acl deny icmp`** commands define an ACL to allow or block ICMP traffic from entering or leaving. For each values describing a flow, the keyword **`any`** can be used to specify a *wildcard* ("don't care") condition. If a value is not specified for a field, a wildcard condition is applied to the field, giving the same effect as if specifying the **`any`** keyword.

The following table describes the command parameters.

Parameter	Value	Meaning
`acl`	*<name>*	ACL name. Use a string of characters or a number.
`icmp`		Defines an ACL for ICMP.
	<SrcAddr/Mask>	This flows source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format ("255.255.0.0").
	<DstAddr/Mask>	This flows destination address and the filtering mask. The same requirements and restrictions for ***<SrcAddr/Mask>*** apply to ***<DstAddr/Mask>***.
	<tos>	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.

Restrictions

When applying an ACL to an interface, implicit deny rule to that ACL is automatically appended. The implicit deny rule denies all traffic. If it is intended to allow all traffic that does not match the specified ACL rules to go through, explicitly define a rule to permit all traffic.

acl permit|deny igmp

Mode

Configure

Format

```
acl <name> permit|deny igmp <SrcAddr/Mask> <DstAddr/Mask> <tos>
```

Description

The **`acl permit igmp`** and **`acl deny igmp`** commands define an ACL to allow or block IGMP traffic from entering or leaving. For each values describing a flow, the keyword **`any`** can be used to specify a *wildcard* ("don't care") condition. If a value is not specified for a field, a wildcard condition is applied to the field, giving the same effect as if specifying the **`any`** keyword.

The following table describes the command parameters.

Parameter	Value	Meaning
`acl`	*<name>*	ACL name. Use a string of characters or a number.
`igmp`		Defines an ACL for IGMP.
	<SrcAddr/Mask>	This flows source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format ("255.255.0.0").
	<DstAddr/Mask>	This flows destination address and the filtering mask. The same requirements and restrictions for ***<SrcAddr/Mask>*** apply to ***<DstAddr/Mask>***.
	<tos>	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.

Restrictions

When applying an ACL to an interface, an implicit deny rule is automatically appended to that ACL. The implicit deny rule denies all traffic. If it is intended to allow all traffic that does not match the specified ACL rules to go through, explicitly define a rule to permit all traffic.

acl permit|deny ip

Mode

Configure

Format

```
acl <name> permit|deny ip <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
```

Description

The **acl permit ip** and **acl deny ip** commands define an Access Control List to allow or block IP traffic from entering or leaving the router. Unlike the more specific variants of the **acl** commands for TCP and UDP, the IP version of the command includes IP-based protocols such as TCP, UDP, ICMP and IGMP. If a value for a field is not specified, the keyword **any** must be entered in it's place to indicate that the value is being bypassed. The exception to this rule is the optional parameters **<tos>** (type of service). **<tos>** is a value from 0 to 15.

The following table describes the command parameters.

Parameter	Value	Meaning
acl	*<name>*	ACL name. Use a string of characters or a number. The string must be less than 100 characters.
ip		Defines an ACL for IP.
	<SrcAddr/Mask>	This flows source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format ("255.255.0.0").
	<DstAddr/Mask>	This flows destination address and the filtering mask. The same requirements and restrictions for ***<SrcAddr/Mask>*** apply to **<DstAddr/Mask>**.
	<SrcPort>	For TCP or UDP, the number of the source TCP or UDP port. This field applies only to TCP or UDP traffic. If the incoming packet is ICMP or another non-TCP or non-UDP packet and there is a specified a source or destination port, the port value is not checked. The device checks only the source and destination IP addresses in the packet. The port numbers of some popular services are already defined as keywords. For example, for Telnet, the port number 23 as well as the keyword **telnet** can be entered.
	<DstPort>	For TCP or UDP, the number of the destination TCP or UDP port. This field applies only to incoming TCP or UDP traffic. The same requirements and restrictions for ***<SrcPort>*** apply to ***<DstPort>***.
	<tos>	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.
	<tos-mask>	Mask value used for the TOS byte. Specify a mask value from 0–255. Default is 30. Specify **any** for any TOS value. The following defined values or names can be used: • dns - DNS port (53) • finger - Finger port (79)

- ftp-cmd - FTP command port (21)
- ftp-data - FTP data port (20)
- http - HTTP (WWW) port (80)
- https - HTTP-Secure (WWW) port (443)
- imap3 - IMAP3 port (220)
- imap4 - IMAP4 port (143)
- lpr - lpr port (515)
- nfs - NFS port (2049)
- nntp - NNTP port (119)
- ntp - NTP port (123)
- pop3 - POP3 port (110)
- portmapper - Portmapper port (111)
- rexec - R-Exec port (512)
- rlogin - R-Login port (513)
- rshell - R-Shell port (514)
- smtp - SMTP port (25)
- snmp - SNMP port (161)
- telnet - Telnet port (23)
- tftp - TFTP port (69)
- x11 - X11 port (6000)

Restrictions

When applying an ACL to an interface, an implicit deny rule is automatically appended to that ACL. The implicit deny rule denies all traffic. To allow all traffic that does not match the specified ACL rules to go through, define a rule to permit all traffic.

acl permit|deny ip protocol

Mode

Configure

Format

```
acl <name> permit|deny ip-protocol <proto-num> <SrcAddr/Mask> <DstAddr/Mask> <tos>
```

Description

The **`acl permit ip-protocol`** and **`acl deny ip-protocol`** commands define an Access Control List to allow or block IP traffic from entering or leaving the router for any protocol type. Unlike the more specific variants of the **`acl`** commands such as **`ip`**, **`tcp`** and **`udp`**, with **`ip-protocol`** version any valid IP protocol type can be specified. Other IP protocols excluding those specified with other **`acl permit|deny`** commands can be specified. For example, to specify an ACL for IP encapsulation in IP, the IPinIP protocol type 4 can be used in the ACL. For each value describing a flow, use the keyword **`any`** to specify a *wildcard* ("don't care") condition. If a value for a field is not specified, the assumed value is a wildcard (the **`any`** keyword).

The following table describes the command parameters.

Parameter	Value	Meaning
`acl`	*<name>*	ACL name. Use a string of characters or a number.
`ip-protocol`		Defines an ACL for IP-Protocol 'n'.
	<proto-num>	IP protocol number of this flow.
	<SrcAddr/Mask>	This flows source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format ("255.255.0.0").
	<DstAddr/Mask>	This flows destination address and the filtering mask. The same requirements and restrictions for ***<SrcAddr/Mask>*** apply to ***<DstAddr/Mask>***.
	<tos>	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.

Restrictions

When applying an ACL to an interface, an implicit deny rule is automatically appended to that ACL. The implicit deny rule denies all traffic. To allow all traffic that does not match the specified ACL rules to go through, define a rule to permit all traffic.

acl permit|deny tcp

Mode

Configure

Format

```
acl <name> permit|deny tcp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
```

Description

The **acl permit tcp** and **acl deny tcp** commands define an ACL to allow or block TCP traffic from entering or leaving. For each of the values describing a flow, the keyword **any** can be used to specify a *wildcard* (“don’t care”) condition. If a value for a field is not specified, a wildcard condition is applied to the field, giving the same effect as specifying the **any** keyword. The exception to this rule is the optional parameters <*tos*> (type of service). <*tos*> is a value from 0 to 15.

The following table describes the command parameters.

Parameter	Value	Meaning
acl	*<name>*	ACL name. Use a string of characters or a number.
tcp		Defines an ACL for TCP.
	<SrcAddr/Mask>	This flows source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format (“255.255.0.0”).
	<DstAddr/Mask>	This flows destination address and the filtering mask. The same requirements and restrictions for ***<SrcAddr/Mask>*** apply to ***<DstAddr/Mask>***.
	<SrcPort>	For TCP or UDP, the number of the source TCP or UDP port. This field applies only to TCP or UDP traffic. The port numbers of some popular services are already defined as keywords. For example, for Telnet, the port number 23 as well as the keyword **telnet** can be entered.
	<DstPort>	For TCP or UDP, the number of the destination TCP or UDP port. This field applies only to incoming TCP or UDP traffic. The same requirements and restrictions for ***<SrcPort>*** apply to ***<DstPort>***.
	<tos>	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.
	<tos-mask>	Mask value used for the TOS byte. Specify a mask value from 0 – 255. Default is 30. Specify **any** for any TOS value.

Restrictions

When applying an ACL to an interface, an implicit deny rule is automatically appended to that ACL. The implicit deny rule denies all traffic. To allow all traffic that does not match the specified ACL rules to go through, define a rule to permit all traffic.

acl permit|deny udp

Mode

Configure

Format

```
acl <name> permit|deny udp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos> <tos-mask>
```

Description

The **acl permit udp** and **acl deny udp** commands define an ACL to allow or block UDP traffic from entering or leaving. For each of the values describing a flow, the keyword **any** can be used to specify a *wildcard* (“don’t care”) condition. If a value for a field is not specified, a wildcard condition is applied to the field, giving the same effect as specifying the **any** keyword. The exception to this rule is the optional parameters ***<tos>*** (type of service). ***<tos>*** is a value from 0 to 15.

The following table describes the command parameters.

Parameter	Value	Meaning
acl	*<name>*	ACL name. Use a string of characters or a number.
udp		Defines an ACL for UDP.
	<SrcAddr/Mask>	This flows source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format (“255.255.0.0”).
	<DstAddr/Mask>	This flows destination address and the filtering mask. The same requirements and restrictions for ***<SrcAddr/Mask>*** apply to **<DstAddr/Mask>**.
	<SrcPort>	For TCP or UDP, the number of the source TCP or UDP port. This field applies only to TCP or UDP traffic. The port numbers of some popular services are already defined as keywords. For example, for Telnet, the port number 23 as well as the keyword **telnet** can be entered.
	<DstPort>	For TCP or UDP, the number of the destination TCP or UDP port. This field applies only to incoming TCP or UDP traffic. The same requirements and restrictions for ***<SrcPort>*** apply to ***<DstPort>***.
	<tos>	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.
	<tos-mask>	Mask value used for the TOS byte. Specify a mask value from 0 – 255. Default is 30. Specify **any** for any TOS value.

Restrictions

When applying an ACL to an interface, an implicit deny rule is automatically appended to that ACL. The implicit deny rule denies all traffic. To allow all traffic that does not match the specified ACL rules to go through, define a rule to permit all traffic.

acl show

Mode

Enable

Format

```
acl show [aclname <string>|all]
```

Description

The **acl show** command is to display the ACLs currently configured.

The following table describes the command parameters.

Parameter	Value	Meaning
aclname		To display ACLs by name.
	<string>	The ACL name.
	all	Specify **all** to display all ACLs.
port		Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific exit port.
	<port>	Specifies the exit port.

Restrictions

None

Example

The example shows the **acl show all** command.

```
rs# acl show all
ACL aclcon:
Applied Interface(s): none
Applied Port(s): none
Forward Count Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort
TOS TOS-
MASK   Prot Flags
------- ----- --------------     -------------      --------- ---------
--- ----
-----  ---- -----
Permit  0     1.1.1.2/8          anywhere           any       any
any any
       ip
Deny    0     anywhere           anywhere           any       any
any any

Flags: E - Established TCP connections only.

ACL aclhi:
Applied Interface(s): none
Applied Port(s): none
Forward Count Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort
TOS TOS-
MASK   Prot Flags
```

```
------- ----- --------------     -------------      --------- ---------
--- ----
-----  ---- -----
Permit  0     2.1.1.2/8          anywhere           any       any
any any
       ip
Deny    0     anywhere           anywhere           any       any
any any

Flags: E - Established TCP connections only.
```

4 ARP COMMANDS

The **arp** command is to add, display, and clear ARP entries on the device.

4.1 COMMAND SUMMARY

The following table lists the **arp** commands. The sections following the table describe the command syntax for each command.

arp add <IpAddr> mac-addr <MAC-addr> exit-port <port> keep-time <seconds>
arp clear <*host*>|all [interface <string>| all] [port <port>]
arp set unresolve-timer <*num*>
arp show <*IPaddr*>|all [undecoded] [interface <string>| all] [port <port>]

arp add

Mode

Configure

Format

```
arp add <IpAddr> mac-addr <MAC-addr> exit-port <port> keep-time <seconds>
```

Description

The **arp add** command is to manually add ARP entries to the ARP table. By default the device automatically creates ARP entries dynamically. Using the **arp add** command an ARP entry can be created to last a specific amount of time or as a permanent ARP entry. This command exists in both Enable and Configure mode with a slight variation. The **keep-time** option is valid only in Enable mode. The **keep-time** option is to create an ARP entry to last a specific amount of time. The Configure mode **arp add** command version does not use the **keep-time** option. ARP entries created in the Configure mode are permanent ARP entries and they do not have an expiration time. If the exit port is not specified, then packets to the IP address for which the ARP entry is created, are transmitted on all interface ports. If an ARP request is received from the host for which the ARP entry is created, then the exit port is updated with the port on which the ARP request is received, so that subsequent packets are transmitted on one port only.

The following table describes the command parameters.

Parameter	Value	Meaning
add	*<IpAddr>*	The IP address.
mac-addr	*<MAC-addr>*	The host MAC address.
exit-port	*<port>*	The port to add the entry. Specify the port to which the host is connected.
keep-time	<seconds>	The number of seconds this ARP entry remains in the ARP table. A value of 0 defines the entry as a permanent ARP entry.

Note This option is valid only for the Enable mode **arp add** command.

Restrictions

Only permanent ARP entries can be entered using the **arp add** command while in the Configure mode.

arp clear

Mode

Enable

Format

```
arp clear <host>|all [interface <string>| all] [port <port>]
```

Description

The **`arp clear`** command is to manually remove entries from the ARP table. The command removes the dynamic entries and refreshes the permanent entries.

The following table describes the command parameters.

Parameter	Value	Meaning
clear	*<host>*	ARP entry Hostname or IP address to remove.
all		Remove all ARP entries, All ARP entries are deleted from the ARP table.
interface		Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific interface.
	<string>	Specifies the interface name.
	all	Specifies all interfaces.
port		Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific exit port.
	<port>	Specifies the exit port.

Restrictions

None

arp set unresolve-timer

Mode

Configure

Format

```
arp set unresolve-timer <num>
```

Description

The **`arp set unresolve-timer`** command is to specify the frequency for sending out ARP requests to resolve the next hop MAC address. This command configures the timer controlling the interval after which the CPU sends ARP requests, and tries to resolve those ARP entries with traffic stopped in hardware.

The following table describes the command parameters.

Parameter	Value	Meaning
`add unresolve-timer`	*<num>*	Specifies that interval for which ARP requests are sent out. Specify any number greater than or equal to 20. This parameter is in seconds. The default is 5 seconds.

Restrictions

None

arp show

Mode

Enable

Format

```
arp show <IPaddr>|all [undecoded] [interface <string>| all] [port <port>]
```

Description

The **arp show** command displays the entire ARP table.

The following table describes the command parameters.

Parameter	Value	Meaning
show	*<IPaddr>*	Shows the ARP entry for the specified IP address.
	all	Shows all entries in the ARP table.
undecoded		Specify this optional parameter to show MAC addresses in hexadecimal format.
interface	*<string>*	Specify this optional parameter to show only addresses in the ARP table associated with the specific interface.
	all	Specifies all interfaces.

Restrictions

None

Examples

This example shows **arp** entries for all device ports.

```
rs# arp show all
----------------|--------------------------|-----------------------|-----------
 IP Address     |     MAC Address          |     Interface[~Port]  |     Flags
----------------|--------------------------|-----------------------|-----------
1.1.1.1         | 00:02:85:13:bf:20        | int1       ~et.2.1    | Static
1.1.1.2         | 00:00:00:00:00:01        | int1       ~et.2.1    | Dynamic
2.1.1.1         | 00:02:85:13:bf:20        | int2       ~et.2.2    | Static
2.1.1.2         | 00:00:00:00:00:02        | int2       ~et.2.2    | Dynamic
3.1.1.1         | 00:02:85:13:bf:20        | int3       ~et.2.3    | Static
3.1.1.2         | 00:00:00:00:00:03        | int3       ~et.2.3    | Dynamic
4.1.1.1         | 00:02:85:13:bf:20        | int4       ~et.2.4    | Static
4.1.1.2         | 00:00:00:00:00:04        | int4       ~et.2.4    | Dynamic
```

```
5.1.1.1          | 00:02:85:13:bf:20         | int5       ~et.2.5      | Static
```

This example shows **arp** MAC entries for a specific IP address workstation.

```
rs# arp show 1.1.1.2
----------------|--------------------------|------------------------|-----------

 IP Address     |     MAC Address          |     Interface[~Port]   |     Flags

----------------|--------------------------|------------------------|-----------

1.1.1.2          | 00:00:00:00:00:01         | int1       ~et.2.1      | Dynamic
```

This example shows specific port **arp** entries.

```
rs# arp show all port et.2.3
----------------|--------------------------|------------------------|-----------

 IP Address     |     MAC Address          |     Interface[~Port]   |     Flags

----------------|--------------------------|------------------------|-----------

3.1.1.1          | 00:02:85:13:bf:20         | int3       ~et.2.3      | Static

3.1.1.2          | 00:00:00:00:00:03         | int3       ~et.2.3      | Dynamic
```

5 COMMENT COMMANDS

The **comment** command is to add user defined comment lines in the active configuration file.

5.1 COMMAND SUMMARY

The following table lists the **command** commands. The sections following the table describe the command syntax for each command.

comment in <*num*>
comment out <*num*>

comment in

Mode

Configure

Format

`comment in <num>`

Description

The **`comment in`** command is to reactivate a command previously negated. To reactivate a command specify the negated command line number in the parameter **`num`**.

The following table describes the command parameters.

Parameter	Value	Meaning
`out`	*<num>*	Specifies the command line number to activate in the active configuration file. Specify in **`num`** a number starting from 1 up to the number of the last line in the file.

Restrictions

None

comment out

Mode

Configure

Format

```
comment out <num>
```

Description

The **comment out** command is to negate an individual command or set of commands in a configuration file. To negate commands specify the command line numbers in the **num** parameter. When executed, the command is left in the configuration file as a comment. Commenting out a command is also known as *negating* a command.

The following table describes the command parameters.

Parameter	Value	Meaning
out	<num>	Specifies the command line number to negate in the active configuration file. Specify in **num** a number starting from 1 up to the number of the last line in the file.

Restrictions

None

6 CONFIGURE COMMAND

configure

Mode

Enable

Format

```
configure
```

Description

The **`configure`** command transfers the CLI session to the configure mode. Use the configure mode to set and change device parameters. To enter the configure mode type **`config`** at the enable prompt. To exit the configure mode, use the **`exit`** command.

Restrictions

The configure mode can only be entered from the enable mode.

7 COPY COMMAND

copy

Mode

Enable

Format

```
copy active |scratchpad | tftp-server | startup | <filename> | <url> to active | scratchpad |
tftp-server | startup | <filename> | <url>
```

Description

The **copy** command is for copying configuration files. Configuration files can be copied between the device and external hosts using protocols such as TFTP. Within the device, configuration files are copied between the device file system, the scratchpad (configuration database), the active (running) configuration, or the startup configuration. The **copy** command can be used to make configuration file backup copies.

The following table describes the command parameters.

Parameter	Value	Meaning
copy		Copies the configuration file.
	active	Specifies the running configuration file.
	scratchpad	Specifies the configuration file in the scratchpad.
	tftp-server	Specifies the TFTP server.
	startup	Specifies the startup configuration file.
	<filename>	Specifies the name of a file.
	<url>	Specifies a URL: tftp://<host>/<filename>
to		Specifies the destination.

Restrictions

The device does not allow some combinations of source and destination pairs. Files cannot be copied from one TFTP server directly to another TFTP server, or copied from scratchpad to scratchpad. Files cannot be copied directly into the active configuration from anywhere except the scratchpad. All changes to the running system must be through the scratchpad.

8 DHCP COMMAND

dhcp global set relay-agent giaddr

Mode

Configure

Format

```
dhcp global set relay-agent giaddr <IPaddr> [threshold <num>]
```

Description

The **`dhcp global set-relay-agent`** command is to configure the device to run a relay agent.

The following table describes the command parameters.

Parameter	Value	Meaning
`giaddr`	`<IPaddr>`	The next configuration server destination IP address. The IP address format is x.x.x.x.
`[threshold]`	`<num>`	The threshold is set in seconds. The default is 0.

Restrictions

None

9 ERASE COMMAND

erase

Mode

Configure

Format

```
erase scratchpad|startup
```

Description

The **erase scratchpad** command erases the device command scratchpad or startup file contents.

The following table describes the command parameters.

Parameter	Value	Meaning
scratchpad		Erases the scratchpad contents. The scratchpad contains configuration commands entered but have not yet been activated.
startup		Erases the Startup configuration contents. The device uses the Startup configuration to configure itself when rebooting. After erasing the Startup configuration, and immediately rebooting, the device can restart without any configuration information.

Restrictions

The **erase** commands do not delete other types of files.

10 EXIT COMMAND

exit

Mode

All modes

Format

```
exit
```

Description

The **exit** command exits the current CLI mode to the previous mode. For example, if in the Enable mode, **exit** returns to the User mode. If in Configure mode, **exit** returns to Enable mode. If in User mode, **exit** closes the CLI session and logs off the device.

Restrictions

None

11 FILTER COMMANDS

The **filters** commands are to create and apply the following types of security filters:

- Address filters block traffic based on a frame source MAC address, destination MAC address, or both. Address filters are always configured and applied on the input port.
- Static entry filters allow or force traffic to go to a set of destination ports based on a frame source MAC address, destination MAC address, or both. Static entry filters are always configured and applied on the input port. Source static entry filters, destination static entry filters, and flow static entry filters can be configured. Source static entry filters allow or disallow frames based on their source MAC address; destination static entry filters allow or disallow frames based on their destination MAC address. Flow static entries allow or disallow traffic based on their source and destination MAC addresses.
- Port-to-address lock filters "lock" a port or set of ports, disallowing them access to other ports.
- Secure port filters shut down Layer 2 access to the device from a specific port or drop all Layer 2 packets received by a port. Used by themselves, secure ports secure unused device ports. When used in conjunction with static entry filters, secure ports drop all received or sent traffic (depending on the static entry filter) except traffic forced to or from the port by the static entry filter.

11.1 COMMAND SUMMARY

The following table lists the **filters** commands. The sections following the table describe the command syntax for each command.

filters add address-filter name *<name>* source-mac *<MACaddr>* source-mac-mask *<MACaddr>* dest-mac *<MACaddr>* dest-mac-mask *<MACaddr>* vlan *<VLAN-num>* in-port-list *<port-list>*
filters add port-address-lock name *<name>* source-mac *<MACaddr>* vlan *<VLAN-num>* in-port-list *<port-list>*
filters add static-entry name *<name>* restriction allow|disallow source-mac *<MACaddr>* source-mac-mask *<MACaddr>* dest-mac *<MACaddr>* dest-mac-mask *<MACaddr>* vlan *<VLAN-num>* in-port-list *<port-list>* out-port-list *<port-list>*
filters show address-filter [all-source|all-destination|all-flow] [source-mac <MACaddr> dest-mac *<MACaddr>*] [ports *<port-list>*] [vlan *<VLAN-num>*]
filters show port-address-lock [ports *<port-list>*] [vlan *<VLAN-num>*] [source-mac *<MACaddr>*]
filters show static-entry [all-source|all-destination|all-flow] ports *<port-list>* vlan *<VLAN-num>* [source-mac *<MACaddr>* dest-mac *<MACaddr>*]

filters add address-filter

Mode

Configure

Format

```
filters add address-filter name <name> source-mac <MACaddr> source-mac-mask <MACaddr>dest-mac
<MACaddr> dest-mac-mask <MACaddr> vlan <VLAN-num> in-port-list <port-list>
```

Description

The **`filters add address-filter`** command blocks traffic based on a frame source MAC address **`source-mac`**, destination MAC address **`dest-mac`**, or a flow (specified using both a source MAC address and a destination MAC address).

The following table describes the command parameters.

Parameter	Value	Meaning
`name`	*<name>*	Specifies the filter name. This parameter must be less than 25 characters.
`source-mac`	*<MACaddr>*|`any`	Specifies the source MAC address. Specify **`any`** to allow any MAC address as the **`source-mac`**. Use this option for source or flow address filters.
`source-mac-mask`	*<MACaddr>*	Specifies the source MAC Mask address. Use this option for source or flow address filters.
`dest-mac`	*<MACaddr>*|`any`	Specifies the destination MAC address. Specify **`any`** to allow any MAC address as the **`dest-mac`**. Use this option for destination or flow address filters.
`dest-mac-mask`	*<MACaddr>*	Specifies the destination MAC Mask address. Use this option for destination or flow static entries.
`vlan`	*<VLAN-num>*|`any`	Specifies the VLAN. Specify **`any`** to allow any VLAN.
`in-port-list`	*<port-list>*	Specifies the ports to apply the filter.

Restrictions

Apply flow filters (specified using both a source MAC address and a destination MAC address) only to ports using flow-based bridging.

filters add port-address-lock

Mode

Configure

Format

```
filters add port-address-lock name <name> source-mac <MACaddr> vlan <VLAN-num>in-port-list
<port-list>
```

Description

The **`filters add port-address-lock`** command locks a user (identified by the user MAC address) to a specific port or set of ports. The source MAC address can only reach stations and ports connected to a port specified by **`in-port-list`**.

The following table describes the command parameters.

Parameter	Value	Meaning
`name`	*<name>*	Specifies the lock filter name. This parameter must be less than 25 characters.
`source-mac`	*<MACaddr>*	Specifies the source MAC address.
`vlan`	*<VLAN-num>*	Specifies the VLAN.
`in-port-list`	*<port-list>*	Specifies the ports to apply the lock.

Restrictions

None

filters add static-entry

Mode

Configure

Format

```
filters add static-entry name <name> restriction allow|disallow source-mac <MACaddr> source-mac-mask <MACaddr> dest-mac <MACaddr> dest-mac-mask <MACaddr> vlan <VLAN-num> in-port-list <port-list> out-port-list <port-list>
```

Description

The **filters add static-entry** command allows, disallows, or forces traffic to go to a set of destination ports based on a frame source MAC address **(source-mac)**, destination MAC address **(dest-mac)**, or a flow (specified using both a source MAC address and a destination MAC address).

The following table describes the command parameters.

Parameter	Value	Meaning
name	*<name>*	Specifies the static-entry filter name. This parameter must be less than 25 characters.
restriction		Specifies the static entry forwarding behavior, which can be one of the following keywords:
	allow	Allows packets to go to the set of ports specified by **out-port-list**.
	disallow	Prohibits packets from going to the set of ports specified by **out-port-list**.
source-mac	*<MACaddr>*|any	Specifies the source MAC address. Specify **any** to allow any MAC address as the **source-mac**. Use this option for source or flow static entries.
source-mac-mask	*<MACaddr>*	Specifies the source MAC address. Use this option for source or flow static entries. The format is ff:ff:ff:ff:ff:ff.
dest-mac	*<MACaddr>*|any	Specifies the destination MAC address. Specify **any** to allow any MAC address as the **dest-mac**. Use this option for destination or flow static entries.
vlan	*<VLAN-num>*|any	Specifies the VLAN number. Specify **any** to allow any VLAN. The VLAN number is between 1 and 4095.
dest-mac-mask	*<MACaddr>*	Specifies the destination MAC address. Use this option for destination or flow static entries. The format is ff:ff:ff:ff:ff:ff.
in-port-list	*<port-list>*	Specifies the ports to apply the static entry.
out-port-list	*<port-list>*	Specifies the ports to allow, disallow, or force packets.

Restrictions

Apply flow filters (specified using both a source MAC address and a destination MAC address) only to ports using flow-based bridging.

filters show address-filter

Mode

Enable

Format

```
filters show address-filter [all-source|all-destination|all-flow] [source-mac <MACaddr> dest-mac <MACaddr>] [ports <port-list>] [vlan <VLAN-num>]
```

Description

The **filters show address-filter** command displays the address filters currently configured on the device.

The following table describes the command parameters.

Parameter	Value	Meaning
address-filter	all-source| all-destination | all-flow	Specifies filter types to display.
source-mac	*<MACaddr>*	Restricts the display to address filters applied to this source MAC address.
dest-mac	*<MACaddr>*	Restricts the display to address filters applied to this destination MAC address.
ports	ports	Restricts the display to address filters applied to the specified ports.
vlan	*<VLAN-num>*	Restricts the display to address filters applied to the specified VLANs.

Restrictions

The following parameter combinations are not functional:

- **address-filter all-source** and **source-mac*<MACaddr>***
- **address-filter all-destination** and **dest-mac*<MACaddr>***
- **address-filter all-flow** and **source-mac*<MACaddr>***
- **address-filter all-flow** and **dest-mac*<MACaddr>***

filters show port-address-lock

Mode

Enable

Format

```
filters show port-address-lock [ports <port-list>] [vlan <VLAN-num>] [source-mac <MACaddr>]
```

Description

The **`filters show port-address-lock`** command displays the port-address-lock filters currently configured on the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`ports`	*`<port-list>`*	Restricts the display to only those port address locks applied to the specified ports.
`vlan`	*`<VLAN-num>`*	Restricts the display to only those port address locks applied to the specified VLANs.
`source-mac`	*`<MACaddr>`*	Restricts the display to only those port address locks applied to the specified source MAC address.

Restrictions

None

filters show static-entry

Mode

Enable

Format

```
filters show static-entry [all-source|all-destination|all-flow] ports <port-list> vlan <VLAN-num> [source-mac <MACaddr> dest-mac <MACaddr>]
```

Description

The **`filters show static-entry`** command displays the static-entry filters currently configured on the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`static-entry`	`all-source|all-destination |all-flow`	Specifies the types of static entries to be displayed.
`ports`	*`<port-list>`*	Restricts the display to only those static entries applied to the specified ports.
`vlan`	*`<VLAN-num>`*	Restricts the display to only those static entries applied to the specified VLANs.
`source-mac`	*`<MACaddr>`*	Restricts the display to only those static entries applied to the specified source MAC address.
`dest-mac`	*`<MACaddr>`*	Restricts the display to only those static entries applied to this destination MAC address.

Restrictions

None

12 GARP COMMANDS

The **garp** commands are to set and show the timers for the Generic Attribute Registration Protocol (GARP).

12.1 COMMAND SUMMARY

The following table lists the **garp** commands. The sections following the table describe the command syntax for each command.

garp set timers leaveall <*number*>|leave <*number*>|join <*number*>
garp show timers

garp set timers

Mode

Configure

Format

```
garp set timers leaveall <number>|leave <number>|join <number>
```

Description

The **garp set timers** command is to set values for the different GARP timers.

The following table describes the command parameters.

Parameter	Value	Meaning
leaveall	<number>	Specify the **leaveall** timer in milliseconds.
leave	<number>	Specify the **leave** timer in milliseconds. It must be three times more than the **join** timer.
join	<number>	Specify the **join** timer in milliseconds.

Restrictions

None

garp show timers

Mode

Enable

Format

```
garp show timers
```

Description

The **garp show timers** command is to display the GARP timers.

Restrictions

None

Example

This example shows the GARP timers.

```
rs# garp show timers

GARP Timers:
     LeaveAll Timer: 10000 milliseconds
     Leave Timer    : 600 milliseconds
     Join Timer     : 200 milliseconds
```

13 GVRP COMMANDS

The **gvrp** commands are to set parameters for the GARP VLAN Registration Protocol (GVRP).

13.1 COMMAND SUMMARY

The following table lists the **gvrp** commands. The sections following the table describe the command syntax.

gvrp clear statistics <*port*>|all-ports
gvrp enable dynamic-vlan-creation
gvrp enable ports <*port-list*>
gvrp set applicant-status non-participant ports <*port-list*>|all-ports
gvrp set registration-mode forbidden ports <*port-list*>|all-ports
gvrp show applicant-status ports <*port-list*>|all-ports
gvrp show error-statistics <*port-list*>|all-ports
gvrp show registration-mode ports <*port-list*>|all-ports
gvrp show statistics <*port-list*>|all-ports
gvrp show status
gvrp start

gvrp clear statistics

Mode

Enable

Format

`gvrp clear statistics <port>|all-ports`

Description

The **`gvrp clear statistics`** command clears GVRP statistics on specified ports.

The following table describes the command parameters.

Parameter	Value	Meaning
`statistics`	*`<port>`*	Clears GVRP statistics on specified ports.
	`all-ports`	Clears GVRP statistics on all ports.

Restrictions

None

gvrp enable dynamic-vlan-creation

Mode

Configure

Format

```
gvrp enable dynamic-vlan-creation
```

Description

The **gvrp enable dynamic-vlan-creation** command enables VLANs to be dynamically created through GVRP.

Restrictions

None

gvrp enable ports

Mode

Configure

Format

```
gvrp enable ports <port-list>
```

Description

The **gvrp enable ports** command enables GVRP on the specified ports.

The following table describes the command parameter.

Parameter	Value	Meaning
ports	*<port-list>*	Enables GVRP on the specified ports.

Restrictions

None

gvrp set applicant-status

Mode

Configure

Format

```
gvrp set applicant-status non-participant ports <port-list>|all-ports
```

Description

The **gvrp set applicant-status** command sets a port status to non-participant, preventing it from sending GARP PDUs.

The following table describes the command parameters.

Parameter	Value	Meaning
ports	*<port-list>*	Sets specified ports to non-participant status.
	all-ports	Sets all ports to non-participant status.

Restrictions

None

gvrp set registration-mode

Mode

Configure

Format

```
gvrp set registration-mode forbidden ports <port-list>|all-ports
```

Description

The **`gvrp set registration-mode`** command sets ports to forbidden registration mode. This mode de-registers all VLANS on the specified port and prevents any VLAN creation or registration on that port.

The following table describes the command parameters.

Parameter	Value	Meaning
`ports`	*`<port-list>`*	Sets specified ports to forbidden registration mode.
	`all-ports`	Sets *all* ports to forbidden registration mode.

Restrictions

None

gvrp show applicant-status

Mode

Enable

Format

```
gvrp show applicant-status ports <port-list>|all-ports
```

Description

The **gvrp show applicant-status** command displays the applicant port status.

The following table describes the command parameter.

Parameter	Value	Meaning
ports	*<port-list>*	Specifies for which ports the applicant status is displayed.
	all-ports	Specifies that the applicant status is displayed for *all* ports.

Restrictions

None

gvrp show error-statistics

Mode

Enable

Format

```
gvrp show error-statistics <port-list>|all-ports
```

Description

The **`gvrp show error-statistics`** command displays the GVRP port errors.

The following table describes the command parameters.

Parameter	Value	Meaning
`error statistics`	*`<port-list>`*	Specifies for which ports the GVRP errors are displayed.
	`all-ports`	Specifies that GVRP errors is displayed for *all* ports.

Restrictions

None

gvrp show registration-mode

Mode

Enable

Format

```
gvrp show registration-mode ports <port-list>|all-ports
```

Description

The **gvrp show registration-mode** command displays whether the ports are in normal registration mode, fixed registration mode, or forbidden registration mode.

The following table describes the command parameters.

Parameter	Value	Meaning
ports	*<port-list>*	Specifies for which ports the registration mode are displayed.
	all-ports	Specifies the registration mode is displayed for *all* ports.

Restrictions

None

gvrp show statistics

Mode

Enable

Format

```
gvrp show statistics <port-list>|all-ports
```

Description

The **gvrp show statistics** command displays the port GVRP statistics.

The following table describes the command parameters.

]Parameter	Value	Meaning
statistics	*<port-list>*	Specifies for which ports the GVRP statistics is displayed.
	all-ports	Specifies the GVRP statistics is displayed for *all* ports.

Restrictions

None

gvrp show status

Mode

Enable

Format

```
gvrp show status
```

Description

The gvrp show status command displays the port GVRP status.

Restrictions

None

Example

This example displays a port GVRP status.

```
rs# gvrp show status

GVRP Status
-----------

GVRP is stopped
Dynamic Vlan Creation is Disabled
Ports GVRP enabled on: None
Applicant Mode set to Non-Participant on Ports: None
Registrar Mode set to Forbidden on Ports: None
```

gvrp start

Mode

Configure

Format

```
gvrp start
```

Description

The **gvrp start** command enables GVRP on the device.

Restrictions

None

14 IGMP COMMANDS

The **igmp** commands are to display and set IGMP parameters.

14.1 COMMAND SUMMARY

The following table lists the **igmp** commands. The sections following the table describe the command syntax for each command.

igmp enable vlan *<vlan-name>*
igmp set vlan *<vlan-name>* [host-timeout *<num>*] [querier-timeout *<num>*] [router-timeout *<num>* leave-timeout *<num>*] [filter-ports *<port-list>*] [permanent-ports *<port-list>*]
igmp show vlans
igmp start-snooping

igmp enable vlan

Mode

Configure

Format

```
igmp enable vlan <vlan-name>
```

Description

The **`igmp enable vlan`** command enables IGMP snooping on a specified VLAN. By default, IGMP snooping is disabled on all VLANs.

The following table describes the command parameter.

Parameter	Value	Meaning
`vlan`	*`<vlan-name>`*	The VLAN name where IGMP snooping is to be enabled.

Restrictions

Layer 3 multicasting and layer-2 snooping cannot be run simultaneously on the same VLAN.

igmp set vlan

Mode

Configure

Format

```
igmp set vlan <vlan-name> [host-timeout <num>] [querier-timeout <num>] [router-timeout <num>
leave-timeout <num>] [filter-ports <port-list>] [permanent-ports <port-list>]
```

Description

The **`igmp set vlan`** command is to set parameters for VLAN-based IGMP snooping.

The following table describes the command parameters.

Parameter	Value	Meaning
`vlan`	*<vlan-name>*	VLAN Name.
`host-timeout`	*<num>*	Allows adjusting to long host timeout values that are set for the IGMP querier. The default value is 250 seconds.
`querier-timeout`	*<num>*	Allows adjusting to long timeout values that are set up the IGMP querier. The default value is 260 seconds.
`router-timeout`	*<num>*	Allows adjusting to long timeout values that are set for the routers. Different versions of DVMRP can have different timeouts. The default value is 140 seconds.
`leave-timeout`	*<num>*	Allows quicker timeout if IGMP v2 leave messages are used. The value is nominally 10 seconds.
`filter-ports`	*<port-list>*	Allows forced filtering of certain ports from Multicast data. Setting ports as filter ports ensures that no host there will join any memberships. A port can optionally be either a permanent port or a filter port, but not both.
`permanent-ports`	*<port-list>*	Allows forcing of Multicast data if present on certain ports. A port can be either a permanent port or a filter port, but not both.

Restrictions

None

igmp show vlans

Mode

Enable

Format

```
igmp show vlans [detail] [name <name>] [timers]
```

Description

The **`igmp show vlans`** command displays port, querier, Multicast group, and group membership information for each VLAN. When running IGMP snooping on a VLAN by using the **`igmp start-snooping`** command, use the **`igmp show vlans`** command to view the resulting statistics.

The following table describes the command parameters.

Parameter	Value	Meaning
`detail`		Displays all IGMP membership information.
`name`	*<name>*	Displays IGMP membership information for the specified VLAN.
`timers`		Displays all IGMP L2 snooping related timers.

Restrictions

None

igmp start-snooping

Mode

Configure

Format

```
igmp start-snooping
```

Description

The **igmp start-snooping** command starts IGMP snooping on enabled VLANs. IGMP snooping allows the switch on a VLAN to determine the following:

- IGMP querier ports on the VLAN
- Multicast groups on the VLAN
- VLAN ports that belong to Multicast groups by monitoring L2 traffic on the VLAN

This task is independent of L3 Multicasting.

Restrictions

None

15 INTERFACE COMMANDS

The **interface** commands are to create IP interfaces, add network mask and broadcast address information to existing IP interfaces, and display configuration information for IP interfaces.

15.1 COMMAND SUMMARY

The following table lists the **interface** commands. The sections following the table describe the command syntax for each command.

interface create ip *<interface-name>* address-netmask *<ipAddr-mask>* [broadcast *<ipaddr>*] vlan *<name>*|port *<port>* [output-mac-encapsulation *<MACencap>*] [up|down] [mac-addr *<MACaddr-spec>*
interface show ip *<InterfaceName>* |all [brief]

interface create ip

Mode

Configure

Format

```
interface create ip <interface-name> address-netmask <ipAddr-mask> [broadcast <ipaddr>] vlan
<name>|port <port> [output-mac-encapsulation <MACencap>] [up|down] [mac-addr <MACaddr-spec>
```

Description

The **interface create ip** command creates and configures an IP interface. IP interface configuration can include information such as the interface name, IP address, netmask, broadcast address, and so on.

The device has a pre-allocated a pool of 64 MAC addresses. By default, each new IP interface is automatically configured with the lowest MAC address in the pool (the "base" MAC address).

Interfaces on the device are logical interfaces. Therefore, an interface can be associated with a single port or with multiple ports.

- To associate an interface with a single port, use the **port** option with the **interface create** command.
- To associate an interface with multiple ports, first create an IP VLAN and add ports to it, then use the **vlan** option with the **interface create** command.

Note Use either the **port** option or the **vlan** option with the **interface create** command.

The following table describes the command parameters.

Parameter	Value	Meaning
ip	*<InterfaceName>*	The IP interface Name; for example, int4.
address-netmask	*<ipAddr-mask>*	The interface IP address and netmask. To specify the address and mask use the traditional format (example: 10.1.2.3/255.255.0.0). If an address is specified without mask information, the device uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).
broadcast	*<ipAddr>*	The broadcast interface IP address. To specify the address use the traditional format (example: 10.1.2.3/255.255.0.0). If an address is specified without mask information, the device uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).
vlan	*<name>*	VLAN name associated with this interface.
port	*<port>*	Port associated with this interface.
up		Sets the interface state to up. (This is the default state.)
down		Sets the interface state to down.
output-mac-encapsulation	*<MACencap>*	The output MAC encapsulation associated with this interface. One of the following options can be specified:
	ethernet_ii	The default.
	ethernet_snap	

mac-addr	auto	Sets the MAC address for this interface.

Restrictions

None

interface show ip

Mode

Enable

Format

```
interface show ip <InterfaceName> | all [brief]
```

Description

The **`interface show ip`** command displays IP interface configuration information.

Note The same information can be displayed using the **`ip show interfaces`** command.

The following table describes the command parameters.

Parameter	Value	Meaning
`ip`	*<InterfaceName>* `all`	IP interface name; for example, int4. Specify **`all`** to display configuration information about all device IP interfaces.
`brief`		Displays a brief interface summary in tabular form.

Restrictions

None

Example

This example shows the IP interface configuration information.

```
rs# interface show ip all
IP Interface table
------------------
Interface qa
    Admin State:          up
    Operational State:    up
    Capabilities:         <BROADCAST,SIMPLEX,MULTICAST>
    Configuration:
       VLAN:
       Ports:             et.2.2
       MTU:               1500
       MAC Encapsulation: ETHERNET_II
       MAC Address:       00:12:34:56:78:00
       IP Address:        16.1.1.3/8  (broadcast: 16.255.255.255)
Interface wa
    Admin State:          up
    Operational State:    up
    Capabilities:         <BROADCAST,SIMPLEX,MULTICAST>
    Configuration:
       VLAN:
       Ports:             et.2.10
       MTU:               1500
       MAC Encapsulation: ETHERNET_II
```

16 IP COMMANDS

The **ip** commands are to configure and display IP characteristics.

16.1 COMMAND SUMMARY

The following table lists the **ip** commands. The sections following the table describe the command syntax for each command.

ip add route <*ipAddr-mask*>|default gateway <*hostname-or-IPaddr*> [host] [interface <*hostname-or-IPaddr*>] [reject]
ip disable forwarding | proxy-arp
ip helper-address interface <*interface-name*> <*helper-address*> |all-interfaces [<*udp-port#*>]
ip-router global set router-id <*ipAddr*>
ip show connections [no-lookup]
ip show helper-address
ip show interfaces *[*<*interface-name*>] [brief]
ip show routes
ip show routes show-arps
ip show routes show-multicast
ip show routes show-protocol default|direct|ospf|rip|static
ip show routes show-summary

ip add route

Mode

Configure

Format

```
ip add route <ipAddr-mask>|default gateway <hostname-or-IPaddr> [host] [interface <hostname-or-IPaddr>] [reject]
```

Description

The **ip add route** command creates a static route entry in the route table. The static route can be a default route, a route to a network, or a route to a specific host.

The following table describes the command parameters.

Parameter	Value	Meaning
route	*<ipAddr-mask>*	The destination IP address and netmask. The address and mask information is specified using the traditional format (example: 10.1.2.3/255.255.0.0). If an address is specified without mask information, the device uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C).
gateway	*<hostname-or-Ipaddr>*	The next hop router IP address or hostname for this route.
Host		Specifies that this route is a route to a host.
interface	*<hostname-or-IPaddr>*]	The next hop interface associated with this route. When this option is specified, gateways are only considered valid when they are on one of these interfaces.
Preference	*<num>*	The static route preference. The preference controls how this route competes with routes from other protocols. The parameter takes a value between 0 - 255. The default preference is 60.
reject		If specified, install this route as a reject route. Instead of forwarding a packet like a normal route, reject routes cause packets to be dropped and unreachable messages to be sent to the packet originator.

Restrictions

None

ip disable

Mode

Configure

Format

```
ip disable forwarding | proxy-arp
```

Description

The **`ip disable`** command is to disable particular features enabled by default on the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`disable`		Feature to disable.
	`forwarding`	Disable all IP packet forwarding.
	`proxy-arp`	Disable proxy ARP on all interfaces.

Restrictions

None

ip helper-address interface

Mode

Configure

Format

```
ip helper-address interface <interface-name> <helper-address>|all-interfaces [<udp-port>]
```

Description

The **ip helper-address** command is to forward specific UDP broadcast from one interface to another. Broadcast packets from one interface are not forwarded (routed) to another interface. However, some applications use UDP broadcast to detect the availability of a service. Other services, for example BOOTP/DHCP, require broadcast packets to be routed so that they can provide services to clients on another subnet. An IP helper can be configured on each interface to have UDP broadcast packets forwarded to a specific host for a specific service or forwarded to all other interfaces.

The **ip helper-address** command is to specify a UDP port number for which UDP broadcast packets with that destination port number are forwarded. By default, if no UDP port number is specified, the device forwards UDP broadcast packets for the following six services:

- BOOTP/DHCP (port 67 and 68)
- DNS (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- TACACS Server (port 49)
- Time Service (port 37)

The following table describes the command parameters.

Parameter	Value	Meaning
interface	*<interface-name>*	IP interface name where UDP broadcast is to be forwarded to the helper address.
	<helper-address>| all-interfaces	Host Address where UDP broadcast packets are forwarded. If **all-interfaces** is specified, UDP broadcast packets are forwarded to all interfaces except the interface on which the broadcast packet is received.
	<udp-port>	The broadcast packet destination UDP port number to forward. If not specified, packets for the six default services are forwarded to the helper address.

Restrictions

If an interface name is specified, the name must belong to an existing IP interface.

ip-router global set router-id

Mode

Configure

Format

```
ip-router global set router-id <ipAddr>
```

Description

The **ip-router global set router-id** command is to set the router ID for OSPF.

The following table describes the command parameters.

Parameter	Value	Meaning
router-id	*<ipAddr>*	The most preferred address is any address other than 127.0.0.1 on the loopback interface. If there is no secondary address on the loopback interface, then the default router id is set to the address of the first interface which is in the up state that the device encounters. The address of a non point-to-point is preferred over the local address of a point-to-point interface.

Restrictions

None

ip show connections

Mode

Enable

Format

```
ip show connections [no-lookup]
```

Description

The **`ip show connections`** command displays all existing TCP and UDP connections to the device as well as TCP/UDP services available on the device.

Note By default, when displaying an IP address, this command attempts to do a reverse DNS lookup to look for the hostname associated with the IP address and display the hostname instead.

Restrictions

None

Example

This example shows all existing TCP and UDP connections and services on the device.

```
rs# ip show connections

Proto Recv-Q Send-Q    Local Address            Foreign Address      (state)
                                                                            ---
-- ------ ------ ------------------       --------------------    ------
tcp     0      0                *:Echo                     *:       * listen
tcp     0      0                *:telnet                   *:       * listen
tcp     0      0    176.243.37.87:telnet     176.220.100.12:    1679 established
udp     0      0                 *:bootp_strap      *:*
udp     0      0                 *:bootp_client     *:*
udp     0      0                 *:tftp             *:*
udp     0      0                 *:snmp             *:*
```

ip show helper-address

Mode

Enable

Format

```
ip show helper-address [<interface-name>]
```

Description

The **ip show helper-address** command displays the IP helper addresses configuration on the system. By specifying the optional parameter, **<interface-name>**, the IP helper addresses configured for that interface is displayed. If the command is executed without specifying an interface name then the IP helper address configuration of all interfaces are displayed.

The following table describes the command parameters.

Parameter	Value	Meaning
helper-address	*<interface-name>*	IP interface name to display any configured IP helper addresses.

Restrictions

If an interface name is specified, the name must belong to an existing IP interface.

Example

This example shows the IP helper addresses configuration on the system.

```
rs# ip show helper-address

Interface     IP address     Helper Address
---------     ----------     --------------
int1          1.1.1.1           none
int2          2.1.1.1           none
int3          3.1.1.1           none
int4          4.1.1.1           none
int5          5.1.1.1           none
int10         10.1.1.1          none
int50         50.1.1.1          none
```

ip show interfaces

Mode

Enable

Format

```
ip show interfaces [<interface-name>] [brief]
```

Description

The **ip show interfaces** command displays the IP interface configuration. If the command is issued without specifying an interface name then all the IP interfaces configurations are displayed. This command displays the same information as the **interface show ip** command.

The following table describes the command parameters.

Parameter	Value	Meaning
interfaces	*<interface-name>*	The IP interface Name; for example, rs4. If an interface name is not specified, the device displays all the IP interfaces.
brief		Displays a brief interface summary in tabular form.

Restrictions

If an interface name is specified, the name must belong to an existing IP interface.

Example

This example shows the device IP interface configuration.

```
rs# ip show interfaces
IP Interface table
------------------
Interface int1
    Admin State:          up
    Operational State:    up
    Capabilities:         <BROADCAST,SIMPLEX,MULTICAST>
    Configuration:
       VLAN:
       Ports:             et.2.1
       MTU:               1500
       MAC Encapsulation: ETHERNET_II
       MAC Address:       00:02:85:13:bf:20
       IP Address:        1.1.1.1/8  (broadcast: 1.255.255.255)
       IP Address:        2.1.1.1/8  (broadcast: 2.255.255.255)
Interface int3
    Admin State:          up
    Operational State:    up
    Capabilities:         <BROADCAST,SIMPLEX,MULTICAST>
    Configuration:
       VLAN:
       Ports:             et.2.3
       MTU:               1500
       MAC Encapsulation: ETHERNET_II
       MAC Address:       00:02:85:13:bf:20
       IP Address:        3.1.1.1/8  (broadcast: 3.255.255.255)
```

ip show routes

Mode

Enable

Format

```
ip show routes
```

Description

The **ip show routes** command displays the IP routing table routes.

Restrictions

None

Example

This example shows IP routing table routes.

```
rs# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.0.0.0/8            directly connected   Direct    int1
2.0.0.0/8            directly connected   Direct    int2
3.0.0.0/8            directly connected   Direct    int3
4.0.0.0/8            directly connected   Direct    int4
5.0.0.0/8            directly connected   Direct    int5
35.0.0.0/8                                Static
50.0.0.0/8           directly connected   Direct    int50
```

ip show routes show-arps

Mode

Enable

Format

```
ip show routes show-arps
```

Description

The **`ip show routes show-arps`** command displays the IP routing table containing ARP entries.

Restrictions

None

Example

This example shows IP routing table containing ARP entries.

```
rs# ip show routes show-arps

Destination          Gateway              Owner     Netif
                                                          -----------
------               -----     -----
0.0.0.0/0            176.243.1.1          Static    reshet
16.0.0.0/8           directly connected   Direct    qa
16.1.1.3             00:12:34:56:78:00    -         qa
40.0.0.0/8           directly connected   Direct    wa
40.1.1.1             00:12:34:56:78:00    -         wa
70.0.0.0/8           directly connected   Direct    rri
70.1.1.1             00:12:34:56:78:00    -         rri
90.0.0.0/8           directly connected   Direct    hamesh
90.1.1.1             00:12:34:56:78:00    -         hamesh
95.0.0.0/8           directly connected   Direct    fs
95.1.1.1             00:12:34:56:78:00    -         fs
176.243.0.0/16       directly connected   Direct    reshet
176.243.37.87        00:12:34:56:78:00    -         reshet
```

ip show routes show-multicast

Mode

Enable

Format

```
ip show routes show-multicast
```

Description

The **ip show routes show-muticast** command displays the IP routing table containing Multicast entries.

Restrictions

None

Example

This example shows IP routing table containing Multicast entries.

```
rs# ip show routes show-multicast

Destination          Gateway              Owner     Netif
-----------           ------              -----     -----
0.0.0.0/0            176.243.1.1          Static    reshet
16.0.0.0/8           directly connected   Direct    qa
40.0.0.0/8           directly connected   Direct    wa
70.0.0.0/8           directly connected   Direct    rri
90.0.0.0/8           directly connected   Direct    hamesh
95.0.0.0/8           directly connected   Direct    fs
176.243.0.0/16       directly connected   Direct    reshet
```

ip show routes show-protocol

Mode

Enable

Format

```
ip show routes show-protocol default|direct|ospf|rip|static
```

Description

The **`ip show routes show-protocol`** command displays the IP routing table containing the routes based on specified protocols.

The following table describes the command parameters.

Parameter	Value	Meaning
`show-protocol`		Shows only the IP routes that belong to one of these specified protocols:
	`default`	Shows all default routes.
	`direct`	Shows all direct routes.
	`ospf`	Shows all OSPF (Open Shortest Path First) routes.
	`rip`	Shows all RIP (Routing Information Protocol) routes.
	`static`	Shows all manually defined routes.

Restrictions

None

Example

This example shows all direct routes on the IP routing table.

```
rs# ip show routes show-protocol direct

Routes belonging to Direct :

Destination          Gateway              Owner     Netif
-----------          ------               -----     -----
16.0.0.0/8           directly connected   Direct    qa
40.0.0.0/8           directly connected   Direct    wa
70.0.0.0/8           directly connected   Direct    rri
90.0.0.0/8           directly connected   Direct    hamesh
95.0.0.0/8           directly connected   Direct    fs
176.243.0.0/16       directly connected   Direct    reshet

rs# ip show routes show-protocol static
Routes belonging to Static :

Destination          Gateway              Owner     Netif
-----------           ------              -----     -----
0.0.0.0/0            176.243.1.1          Static    reshet
```

ip show routes show-summary

Mode

Enable

Format

```
ip show routes show-summary
```

Description

The **ip show routes show-summary** command displays the IP routing table containing a summary of all route entries.

Restrictions

None

Example

This example shows the IP routing table containing a summary of all route entries.

```
rs# ip show routes show-summary

Summary of Routes by owner:
---------------------------

Owner of the routes      Number of routes
-------------------      ----------------
Direct :                       6
Static :                       1
```

17 L2-TABLES COMMANDS

The **l2-tables** commands are to display various L2 tables related to MAC addresses.

17.1 COMMAND SUMMARY

The following table lists the **l2-tables** commands. The sections following the table describe the command syntax for each command.

l2-tables show all-macs [verbose] [vlan <*VLAN-num*>] [multicast]
l2-tables show igmp-mcast-registrations [vlan <*VLAN-num*>]
l2-tables show mac <*MACaddr*> vlan <*VLAN-num*>
l2-tables show mac-table-stats
l2-tables show vlan-igmp-status vlan <*VLAN-num*>

l2-tables show all-macs

Mode

User or Enable

Format

```
l2-tables show all-macs [verbose] [vlan <VLAN-num>] [multicast]
```

Description

The **`l2-tables show all-macs`** command displays the MAC addresses currently in the device L2 tables. The information displayed can be programmed to include VLAN, source MAC address, destination MAC address or Multicast.

The following table describes the command parameters.

Parameter	Value	Meaning
`vlan`	*<VLAN-num>*	Displays only MAC addresses in the specified VLAN.
`multicast`		Displays only Multicast and broadcast addresses.
`verbose`		Shows detailed information for each MAC address entry.

Restrictions

None

Example

This example shows the number of MAC entries.

```
rs# l2-tables show all-macs

Statistics Summary
---------------------
Total number of unique MACs found         200
MACs that reside on a port as a source    200
Multicasts (from source MACs)               0
```

l2-tables show igmp-mcast-registrations

Mode

User or Enable

Format

```
l2-tables show igmp-mcast-registrations [vlan <VLAN-num>]
```

Description

The **`l2-tables show igmp-mcast-registrations`** command displays the Multicast MAC addresses that IGMP has registered with the L2 tables. The device forwards the Multicast MAC addresses only to the ports that IGMP specifies.

The following table describes the command parameters.

Parameter	Value	Meaning
`vlan`	*<VLAN-num>*	Displays only the Multicast MAC addresses registered for the specified VLAN.

Restrictions

None

l2-tables show mac

Mode

User or Enable

Format

`l2-tables show mac <MACaddr> vlan <VLAN-num>`

Description

The **`l2-tables show mac`** command displays the VLAN and the port number on which the specified MAC address reside.

The following table describes the command parameters.

Parameter	Value	Meaning
`mac`	*<MACaddr>*	The device MAC address. The address can be specified in the following format: xx:xx:xx:xx:xx:xx
`vlan`	*<VLAN-num>*	Displays the MAC address for this VLAN.
`verbose`		Shows detailed information for each MAC address entry.

Restrictions

None

l2-tables show mac-table-stats

Mode

User or Enable

Format

```
l2-tables show mac-table-stats
```

Description

The **`l2-tables show mac-table-stats`** command displays statistics for the MAC address tables on the individual ports.

Restrictions

None

Example

This example shows the **`l2-tables show mac-table-stats`** table.

```
rs# l2-tables show mac-table-stats

MAC Address Table - Statistics Summary
--------------------------------------
Current number of learned MAC address: 200
```

l2-tables show vlan-igmp-status

Mode

User or Enable

Format

```
l2-tables show vlan-igmp-status vlan <VLAN-num>
```

Description

The **`l2-tables show vlan-igmp-status`** command shows the Multicast MAC addresses that IGMP has registered with the L2 tables. This command also shows the ports to which the Multicast MAC addresses are forwarded.

Note For IGMP forwarding to occur for a Multicast MAC address, IGMP must be enabled on the VLAN with which the MAC address is associated.

The following table describes the command parameters.

Parameter	Value	Meaning
`vlan`	*<VLAN-num>*	The VLAN number. The VLAN number can be from 1 – 4095.

Restrictions

None

18 LOGOUT COMMAND

logout

Mode

All modes

Format

```
logout
```

Description

The **logout** command ends the CLI session. If there are uncommitted changes in the scratchpad, a message indicates that the changes are not saved and gives an opportunity to cancel the logout and save the changes.

Restrictions

None

19 MULTICAST COMMANDS

The **multicast** commands are to display IP Multicast interfaces information.

19.1 COMMAND SUMMARY

The following table lists the **multicast** commands. The sections following the table describe the command syntax for each command.

multicast show interface [<*ipAddr*>|<*hostname*>]
multicast show mroutes [child <*IPaddr*>] [group <*ipaddr*>] [parent <*IPaddr*>]

multicast show interfaces

Mode

Enable

Format

```
multicast show interface [<ipAddr>|<hostname>]
```

Description

The **multicast show interface** command displays interfaces running IGMP or DVMRP.

Note This command is a superset of the **dvmrp show interface** and **igmp show interface** commands.

The following table describes the command parameters.

Parameter	Value	Meaning
interface	<ipAddr>|<hostname>	Interface IP address or hostname.

Restrictions

None

multicast show mroutes

Mode

Enable

Format

```
multicast show mroutes [child <ipaddr>] [group <ipaddr>] [parent <ipaddr>]
```

Description

The **`multicast show mroutes`** command displays the IP Multicast forwarding table entries. This command lists all the Multicast distribution trees, displaying the parent interface (from where the traffic is coming), and forwarded traffic distribution interfaces. It also displays any cache information available either in hardware forwarding mechanism or in the main processor (for software based forwarding).

Note The cache information can be timed out when not enough traffic is present, but Multicast routes can still be present. Cache information is presented in a number of flows (Layer 4 sessions). Multicast routes stay at least for 5 minutes, while the hardware forwarding mechanism can time out a flow faster.

Looking at a particular group, and/or looking at a particular parent interface, and/or looking at a particular child interface can narrow the search. Multicast routes are not the same as DVMRP routes.

The following table describes the command parameters.

Parameter	Value	Meaning
`child`	*<ipaddr>*	Child interface address.
`group`	*<ipaddr>*	Multicast group address.
`parent`	*<ipaddr>*	Parent interface address.

Restrictions

None

20 NEGATE COMMAND

negate

Mode

Configure

Format

```
negate <cmd-number>|all active-config
```

Description

The **negate** command is to negate one or more commands by specifying the command number as listed by the command show **active-config**. Specific commands or all the commands can be negated from the active running system.

The following table describes the command parameters.

Parameter	Value	Meaning
	<cmd-number>	The number of the command(s) to negate. Use the **show** command to display the command numbers.
all		Negate all the commands.
active-config		Negate the specified command from the active running system.

Restrictions

The specified command number must represent a command that exists.

21 NO COMMAND

no

Mode

Configure

Format

no <*command-to-negate*>

Description

The **no** command is to negate a previously executed command. Following the keyword **no**, the command is specified to negate in its entirety or use the wildcard character **(***) to negate a group of commands. In addition to the **no** command the **negate** command can be used to negate a group of commands using the command number.

The following table describes the command parameters.

Parameter	Value	Meaning
no	<*command*>	The CLI command to be negated. The entire command does not have to be entered. The wildcard character, *, can be used to negate matching commands. For example, if **no acl 100 *** is specied then all commands starting with the words **acl 100** are negated.

Restrictions

The command to negate must already be in the active configuration. A command that is not entered cannot be negated.

22 OSPF COMMANDS

The **ospf** commands sets and displays the Open Shortest Path First (OSPF) routing protocol.

22.1 COMMAND SUMMARY

The following table lists the **ospf** commands. The following table describes the command syntax for each command.

ospf add interface <*interfacename-or-IPaddr*> to-area <*area-id*>|backbone [type broadcast]
ospf create area <*area-id*>|backbone
no ospf start
ospf clear database
ospf set area <*area-id*>|backbone [stub] [stub-cost <*num*>] [authentication-method none] [retransmit-interval <*num*>] [transit-delay <*num*>] [priority <*num*>] [hello-interval <*num*>] [router-dead-interval <*num*>] [poll-interval <*num*>]
ospf set authentication-method none
ospf set hello-interval <*num*>
ospf set interface <*name-or-IPaddr*>|all [state disable|enable] [cost <*num*>] [retransmit-interval <*num*>] [transit-delay <*num*>] [priority <*num*>] [hello-interval <*num*>] [router-dead-interval <*num*>] [poll-interval <*num*>] [authentication-method none]
ospf set poll-interval <*num*>
ospf set priority <*num*>
ospf set retransmit-interval <*num*>
ospf set router-dead-interval <*num*>
ospf set transit-delay <*num*>
ospf show all
ospf show areas <*IPaddr*>|backbone|all
ospf show as-external-lsdb
ospf show database asbr-summary |external| database-summary | network| router|summary|link-id <*ip-addr*>|adv-router <*ip-addr*>

ospf show globals
ospf show interfaces [detail]
ospf show lsa [area-id <*area-id*>] [type router-links|network-links | summary-networks |summary-asbr |as-external] [ls-id <*IPaddr*>] [adv-rtr <*routerID*>]
ospf show neighbor
ospf start

ospf add interface

Mode

Configure

Format

```
ospf add interface <interfacename-or-IPaddr> to-area <area-id>|backbone [type broadcast]
```

Description

The **ospf add interface** command associates an interface with an OSPF area.

The following table describes the command parameters.

Parameter	Value	Meaning
interface	*<interfacename-or-IPaddr>*	An interface name or an IP address.
to-area	*<area-id>*	OSPF area to associate this interface.
	backbone	Backbone area to associate this interface.
type	broadcast	Specifies the interface is broadcast.

Restrictions

None

ospf create area

Mode

Configure

Format

`ospf create area <area-id>|backbone`

Description

The **`ospf create area`** command creates an OSPF area.

The following table describes the command parameters.

Parameter	Value	Meaning
`area`	*`<area-id>`*	The area ID. Area IDs are formatted like IP addresses: *<num>.<num>.<num>.<num>*.
	`backbone`	Specifies that the area being added is the backbone area.

Restrictions

None

no ospf start

Mode

Configure

Format

```
no ospf start
```

Description

The **no ospf start** command stops the OSPF protocol. OSPF is disabled by default on the device.

Restrictions

None

ospf clear database

Mode

Enable

Format

```
ospf clear database
```

Description

The **`ospf clear database`** command clears the OSPF database.

Restrictions

None

ospf set area

Mode

Configure

Format

```
ospf set area <area-id>|backbone [stub] [stub-cost <num>] [authentication-method none]
[retransmit-interval <num>] [transit-delay <num>] [priority <num>] [hello-interval <num>]
[router-dead-interval <num>] [poll-interval <num>]
```

Description

The **`ospf create area`** command sets the parameters for an OSPF area.

The following table describes the command parameters.

Parameter	Value	Meaning
`area`	*<area-id>*	The area ID.
	`backbone`	Specifies that the area being added is the backbone area.
`stub`		Makes this area a stub area.
`stub-cost`		Specifies the cost to be used to add a default route into the area. Specify a number from 1 – 65535.
`authentication-method`		Specifies the authentication method used within the area.
	`none`	Does not use authentication.
`no-summary`		Specifies that this is a full stub area.
`retransmit-interval`	*<num>*	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. Specify a number equal to or greater than 1. The default is 5.
`transit-delay`	*<num>*	The estimated number of seconds required to transmit a link state update over this interface. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.
`priority`	*<num>*	A number between 0 and 255 specifying the priority for becoming the designated router on this interface. When two routers are attached to a network both attempt to become the designated router, the one with the higher priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become a designated router. Specify a number from 0 – 255. The default is 1.
`hello-interval`	*<num>*	The length of time, in seconds, between hello packets sent by the router on this interface. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.
`router-dead-interval`	*<num>*	The number of seconds a router does not receive Hello packets from its neighbor before it declares its neighbor is down. Specify a number from 0 – 255. The default is 4 times the hello interval value.
`poll-interval`	*<num>*	The interval at which OSPF packets are sent, before an adjacency is established with a neighbor. Specify a number equal to or greater than 1. The

	established with a neighbor. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.

Restrictions

None

ospf set authentication-method

Mode

Configure

Format

```
ospf set authentication-method none
```

Description

The **ospf set authentication-method** command specifies the authentication method used.

The following table describes the command parameters.

Parameter	Value	Meaning
authentication-method	none	Does not use authentication.

Restrictions

None

ospf set hello-interval

Mode

Configure

Format

```
ospf set hello-interval <num>
```

Description

The **`ospf set hello-interval`** command sets the interval between hello packet transmissions.

The following table describes the command parameters.

Parameter	Value	Meaning
`hello-interval`	*<num>*	The length of time, in seconds, between hello packet transmissions. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.

Restrictions

None

ospf set interface

Mode

Configure

Format

```
ospf set interface <name-or-IPaddr>|all [state disable|enable] [cost <num>] [retransmit-interval <num>] [transit-delay <num>] [priority <num>] [hello-interval <num>] [router-dead-interval <num>] [poll-interval <num>] [authentication-method none]
```

Description

The **`ospf set interface`** command sets parameters for an OSPF interface.

The following table describes the command parameters.

Parameter	Value	Meaning
`interface`	*<name-or-IPaddr>*	The OSPF interface to set OSPF parameters.
	`all`	Specifies parameters are set for all OSPF interfaces.
`state`	`disable`	Disables OSPF on the interface.
	`enable`	Enables OSPF on the interface.
`cost`	*<num>*	The cost associated with this interface. Specify a number from 1 – 65535. The total cost to get to a destination is calculated by adding up the cost of all interfaces that a packet must cross to reach a destination. The device calculates the default cost of an OSPF interface using the reference bandwidth and the interface bandwidth. The default reference bandwidth is 1000. A VLAN attached to an interface could have several ports of differing speeds. The highest bandwidth port in the associated VLAN represents the interface bandwidth. The cost of an OSPF interface is inversely proportional to this bandwidth. The cost is calculated using the following formula: *Cost* = reference bandwidth * 1,000,000/ *interface bandwidth (in bps)*
`retransmit-interval`	*<num>*	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. Specify a number equal to or greater than 1. The default is 5.
`transit-delay`	*<num>*	The estimated number of seconds required to transmit a link state update over this interface. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.
`priority`	*<num>*	A number between 0 and 255 specifying the priority for becoming the designated router on this interface. When two routers are attached to a network, both attempt to become the designated router, the one with the higher priority becomes the designated router. A router

		whose router priority is set to 0 is ineligible to become a designated router. Specify a number from 0 – 255. The default is 1.
`hello-interval`	*<num>*	The length of time, in seconds, between hello packets sent by the router on this interface. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.
`router-dead-interva`	*<num>*	The number of seconds not hearing a router Hello packets before the router neighbors declare it down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.
`poll-interval`	*<num>*	Before an adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.
`key-chain`	*<num-or-string>*	Identify the key-chain containing the authentication keys.
`authentication-method`		Specifies the authentication method used within the area.
	`none`	Does not use authentication.

Restrictions

None

ospf set poll-interval

Mode

Configure

Format

```
ospf set poll-interval <num>
```

Description

The **ospf set poll-interval** command sets the interval at which OSPF packets are sent before an adjacency is established.

The following table describes the command parameters.

Parameter	Value	Meaning
poll-interval	<num>	Before adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.

Restrictions

None

ospf set priority

Mode

Configure

Format

```
ospf set priority <num>
```

Description

The **`ospf set priority`** command sets the router priority for becoming the designated router.

The following table describes the command parameters.

Parameter	Value	Meaning
`priority`	*<num>*	A number between 0 and 255 specifying the priority for becoming the designated router. When two routers are attached to a network, both attempt to become the designated router, the one with the higher priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become a designated router. Specify a number from 0 – 255. The default is 1.

Restrictions

None

ospf set retransmit-interval

Mode

Configure

Format

```
ospf set retransmit-interval <num>
```

Description

The **ospf set retransmit-interval** command sets the interval between link state advertisement retransmissions for adjacencies.

The following table describes the command parameters.

Parameter	Value	Meaning
retransmit-interval	*<num>*	The number of seconds between link state advertisement retransmissions for adjacencies. Specify a number equal to or greater than 1. The default is 5.

Restrictions

None

ospf set router-dead-interval

Mode

Configure

Format

```
ospf set router-dead-interval <num>
```

Description

The **`ospf set router-dead-interval`** command sets the interval during which a router does not receive hello packets before it considers its neighbor to be down.

The following table describes the command parameters.

Parameter	Value	Meaning
`router-dead-interval`	*<num>*	The number of seconds a router does not receive hello packets before it declares its neighbor to be down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.

Restrictions

None

ospf set transmit-delay

Mode

Configure

Format

```
ospf set transit-delay <num>
```

Description

The **`ospf set transit-delay`** command sets the estimated interval required to transmit a link state update.

The following table describes the command parameters.

Parameter	Value	Meaning
`transit-delay`	*<num>*	The estimated number of seconds required to transmit a link state update. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.

Restrictions

None

ospf show all

Mode

Enable

Format

```
ospf show all
```

Description

The **`ospf show all`** command displays the following OSPF tables:

- Globals
- Timers
- Area
- Interface
- LSA
- Next-hop
- Export policies
- Import policies

Restrictions

None

ospf show areas

Mode

Enable

Format

```
ospf show areas <IPaddr>|backbone|all
```

Description

The **ospf show areas** command displays OSPF areas.

The following table describes the command parameters.

Parameter	Value	Meaning
areas		Displays specified OSPF area information.
	<IPaddr>	The specified area IP address.
	backbone	Backbone area.
	all	All areas.

Restrictions

None

ospf show as-external-lsdb

Mode

Enable

Format

```
ospf show as-external-lsdb
```

Description

The **`ospf show as-external-lsdb`** command displays OSPF Autonomous System (AS) external Link State Advertisements (LSAs) in the database.

Restrictions

None

ospf show database

Mode

Enable

Format

```
ospf show database asbr-summary |external| database-summary | network| router|summary|link-id <ip-addr>|adv-router <ip-addr>
```

Description

The **`ospf show database`** command displays an OSPF database summary.

The following table describes the command parameters.

Parameter	Value	Meaning
`asbr-summary`		Displays ASBR summary link states.
`external`		Displays external link states.
`database-summary`		Displays the database summary.
`network`		Displays network link states.
`router`		Displays router link states.
`summary`		Displays network summary link states.
`link-id`	*<ip-addr>*	Displays link state ID (as an IP address).
`adv-router`	*<ip-addr>*	Displays the advertising router link states.

Restrictions

None

ospf show globals

Mode

Enable

Format

```
ospf show globals
```

Description

The **`ospf show globals`** command displays OSPF global parameters.

Restrictions

None

ospf show interfaces

Mode

Enable

Format

```
ospf show interfaces [detail]
```

Description

The **ospf show interfaces** command displays OSPF interfaces.

Restrictions

None

ospf show lsa

Mode

Enable

Format

```
ospf show lsa [area-id <area-id>] [type router-links|network-links | summary-networks
|summary-asbr |as-external] [ls-id <IPaddr>] [adv-rtr <routerID>]
```

Description

The **ospf show lsa** command is to display link state advertisements, by type. There are five LSA types. All LSAs, except for the **as-external** LSAs are flooded throughout a single area. The **as-external** LSAs are flooded throughout the entire Autonomous System (AS), except through the stub area:

- **router-links** - These LSAs describe the router working connections (interfaces and links). The router generates router link LSAs for each area to which it belongs.
- **network-links** - These LSAs describe all routers attached to the network. These LSAs are generated by the designated router of a broadcast.
- **as-external** - These LSAs describe routes to destinations external to the AS. These LSAs are generated by AS boundary routers.

The following two LSAs describe inter-area routes, and enable routing information condensing at area borders.

Both types are generated by area border routers.

- summary-network - These are summary LSAs that describe routes to the network specified by the LSA ID.
- summary-asbr - These are summary LSAs that describe routes to the AS boundary router specified by the LSA ID.

The following table describes the command parameters.

Parameter	Value	Meaning
area-id	*<area-id>*	Specifies the OSPF area IP address being described.
	router-links	Specifies the router links advertisements. To describe the router interfaces status. Set the LSA ID **(ls-id** field) to the originating router ID.
	network-links	Specifies the network links advertisements. They describe the set of routers attached to the network specified by the LSA ID. Set the LSA ID **(ls-id** field) to the network designated router IP interface address.
	summary-networks	Specifies the summary links advertisements. They describe the set of routers attached to the network specified by the LSA ID. Set the LSA ID **(ls-id** field) to the destination network IP address.
	summary-asbr	Specifies the summary link advertisements. They describe routes to AS boundary routers. Set the LSA ID **(ls-id** field) to the router ID of the AS boundary router being described.
	as-external	Specifies the AS external link advertisements. They describe routes to destinations external to the AS. Set the LSA ID **(ls-id** field) to the destination network IP address.
ls-id	*<IPaddr>*	The LSA ID. It identifies the routing domain part being described by the LSA. Its value depends on the LSA type specified.
adv-rtr	*<routerID>*	Router ID which originated the LSAs.

Restrictions

None

ospf show neighbor

Mode

Enable

Format

```
ospf show neighbor
```

Description

The **`ospf show neighbor`** command displays the OSPF neighbors.

Restrictions

None

ospf start

Mode

Configure

Format

```
ospf start
```

Description

The **ospf start** command starts the OSPF protocol. OSPF is disabled by default on the device.

Restrictions

None

23 PING COMMAND

ping

Mode

Enable

Format

`ping <hostname-or-IPaddr>`

Description

The **`ping`** command tests the connection between the device and an IP host. The ping command sends ICMP echo packets to the specified host.

- If the packets reach the host, the host sends a ping response to the device and the CLI displays messages stating that the host can be reached.
- If the host does not respond, the device assumes the host cannot be reached from the device, and the CLI display messages states that the host did not reply.

The following table describes the command parameters.

Parameter	Value	Meaning
`ping`	*`<hostname-or-IPaddr>`*	The host name or IP address to ping.

Restrictions

None

24 PORTS COMMANDS

The port commands sets and displays the following parameters:

- Port state (enabled or disabled)
- Port auto-negotiation and flow-control operation modes (enable or disable)
- Port duplex operating mode (half duplex or full duplex)
- Port speed operation mode for the 10/100/1000 ports (10-Mbps, 100-Mbps or 1000-Mbps)
- Port mirroring (used for analyzing network traffic)
- Port bmon control (rate limit of Multicast, broadcast and unknown Unicast/Multicast packets)

24.1 COMMAND SUMMARY

The following table lists the **ports** commands. The sections following the table describe the command syntax for each command.

port auto-negotiate enable <*port-list*>|disable <*port-list*>|restart <*port-list*>
port bmon [rate <*number*>] [broadcast enable|disable] [multicast enable|disable] [unknown_unicast enable|disable]
port description <*port-list*> <*desc*>
port disable <*port-list*>|all-ports
port enable <*port-list*>|all-ports
port set <*port-list*>|all-ports [auto-negotiation on|off] [duplex full|half] [flowctl off|enRx|enTx|both] [speed 10Mbps|100Mbps|1000Mbps]
port show auto-negotiate <*port-list*>|all-ports
port show auto-negotiation-capabilities <*port-list*>|all-ports
port show bmon [config] [detail] [port <*port list*>] [stats]
port show description <*port-list*>|all-ports
port show flowctl <*port-list*>|all-ports
port show mirroring-status
port show port-status <*port-list*>|all-ports
port show stp-info <*port-list*>|all-ports
port show vlan-info <*port-list*>|all-ports

port auto-negotiate enable

Mode

Configure

Format

`port auto-negotiate enable <port-list> | disable <port-list> | restart <port-list>`

Description

The **`port auto-negotiate`** command is to enable auto-negotiation on a port, disable auto-negotiation on a port, or restart auto-negotiation on a port. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

The following table describes the command parameters.

Parameter	Value	Meaning
`enable`	*<port-list>*	Enables auto-negotiation on the port or set of ports.
`disable`	*<port-list>*	Disables auto-negotiation on the port or set of ports.
`restart`	*<port-list>*	Restarts auto-negotiation on the port or set of ports.

Restrictions

None

port bmon

Mode

Configure

Format

```
port bmon [rate <number>] [broadcast enable|disable] [multicast enable|disable]
[unknown_unicast enable|disable]
```

Description

The **port bmon** command is to set the rate limit in packets per second and enable/disable the kind of packets that need to be limited broadcast, unknown Multicast and unknown Unicast packets.

This command can be used where excess traffic is degrading performance. This command is used for all ports altogether.

This reduces the risk of the device becoming overloaded by traffic.

The following table describes the command parameters.

Parameter	Value	Meaning
bmon		
rate	*<number>*	The rate limit, in packets per second. After this limit the packets are dropped.
		The range of <*number*> is 512 to 148000. The default value is 1024.
broadcast		Specifies whether broadcasting is enabled.
	enable	Specifies that broadcasting is allowed.
	disable	Specifies that broadcasting is not allowed.
multicast		Specifies whether unknown Multicasting is enabled.
	enable	Specifies that unknown Multicast packets are allowed.
	disable	Specifies that unknown Multicast packets are not allowed.
unknown_unicast		Specifies whether unknown Unicast packets are allowed.
	enable	Specifies that unknown Unicast packets are allowed.
	disable	Specifies that unknown Unicast packets are not allowed.

Restrictions

None

port description

Mode

Configure

Format

```
port description <port-list> <desc>
```

Description

The **`port description`** command is to define a character string description for a port. This is useful for management purposes.

The following table describes the command parameters.

Parameter	Value	Meaning
`description`	*`<port-list>`*	Specifies the port(s). Valid for Ethernet and WAN ports only.
	`<desc>`	Specifies the port description character string. The string must be 125 characters or less.

Restrictions

None

Example

This example shows a port character string description.

```
rs# port show description et.2.2
Port          Description
et.2.2          Work1
```

port disable

Mode

Configure

Format

```
port disable <port-list>|all-ports
```

Description

The **`port disable`** command disables specified ports. Disabled ports do not send or receive traffic. Disable unused ports to prevent network users from connecting to unoccupied but enabled ports on the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`disable`	*`<port-list>`*	Specifies the ports to disabling.

Restrictions

None

port enable

Mode

Configure

Format

`port enable <port-list>|all-ports`

Description

The **`port enable`** command enables specified ports. Enabled ports send or receive traffic.

The following table describes the command parameters.

Parameter	Value	Meaning
`enable`	*`<port-list>`*	Specifies the ports being enabling.

Restrictions

None

port set

Mode

Configure

Format

```
port set <port-list>|all-ports [auto-negotiation on|off] [duplex full|half] [flowctl
off|enRx|enTx|both] [speed 10Mbps|100Mbps|1000Mbps]
```

Description

The parameters can be set with the **`port set`** command depend on the port media type.

The following table describes the command parameters.

Parameter	Value	Meaning
`set`	*`<port-list>`*	Specifies ports to set.
	`all-ports`	The **`all-ports`** keyword applies the settings selected to all the relevant ports.
`auto-negotiation`		Turns on or off auto-negotiation. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control to communicate with each other.
	`on`	Turns on auto-negotiation.
	`off`	Turns off auto-negotiation.
`duplex`		Sets the operating mode.
	`full`	Set the operating mode to full duplex.
	`half`	Set the operating mode to half duplex.
`speed`		Sets the speed on a fast Ethernet or Gigabit Ethernet port.
	`10Mbps`	Sets the line speed capability to 10Mbits/sec.
	`100Mbps`	Sets the line speed capability to 100Mbits/sec.
	`1000Mbps`	Sets the line speed capability to 1000Mbits/sec.
`flowctl`		Sets the flow-control.
	`off`	Turns off flow-control.
	`enRx`	Acts on received PAUSE flow control frames.
	`enTx`	PAUSE flow control frames are allowed to be transmitted.
	`both`	Sets on both above options.

Restrictions

None

port show auto-negotiate

Mode

Enable

Format

```
port show auto-negotiate <port-list> | all-ports
```

Description

The **port show auto-negotiate** command displays auto-negotiation information. This command displays port number, administration status, current status, remote signaling, fault advertised, and faults received.

Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode, and flow control scheme to communicate with each other.

The following table describes the command parameters.

Parameter	Value	Meaning
auto-negotiate	*<port-list>*	Specifies for which ports to display auto-negotiation information
	all-ports	The **all-ports** keyword displays the auto-negotiation information for all device ports.

Restrictions

Asymmetric Pause and Symmetric Pause are not supported.

Example

This example displays auto-negotiation information for all device ports.

```
rs# port show auto-negotiate all-ports
         Auto
Port     Negotiation  Current    Remote         Fault       Fault
         Status       Status     Signalling     Advertised  Received
et.2.1    disabled   disabled     disabled       n/a         n/a
et.2.2    enabled    complete     not detected   disabled    disabled
et.2.3    enabled    complete     not detected   disabled    disabled
et.2.4    enabled    complete     not detected   disabled    disabled
et.2.5    enabled    complete     not detected   disabled    disabled
et.2.6    enabled    complete     not detected   disabled    disabled
et.2.7    enabled    complete     not detected   disabled    disabled
et.2.8    enabled    complete     not detected   disabled    disabled
et.2.9    enabled    in progress  not detected   disabled    disabled
et.2.10   enabled    in progress  not detected   disabled    disabled
et.2.11   enabled    in progress  not detected   disabled    disabled
et.2.12   enabled    in progress  not detected   disabled    disabled
et.2.13   enabled    in progress  not detected   disabled    disabled
et.2.14   enabled    in progress  not detected   disabled    disabled
et.2.15   enabled    in progress  not detected   disabled    disabled
et.2.16   enabled    in progress  not detected   disabled    disabled
et.2.17   enabled    in progress  not detected   disabled    disabled
et.2.18   enabled    in progress  not detected   disabled    disabled
et.2.19   enabled    in progress  not detected   disabled    disabled
```

port show auto-negotiation-capabilities

Mode

Enable

Format

```
port show auto-negotiation-capabilities <port-list> | all-ports
```

Description

The **port show auto-negotiation-capabilities** command displays auto-negotiation capabilities. This command displays a list of port capabilities, advertised capabilities, and any received capabilities from another port.

Auto-negotiate is a process whereby both ports on a connection resolve the best line speed, duplex mode, and flow control scheme to communicate with each other.

The following table describes the command parameters.

Parameter	Value	Meaning
Auto-negotiation-capabilities	*<port-list>*	Specifies for which ports to display auto-negotiation capabilities.
	all-ports	The **all-ports** keyword displays the auto-negotiation capabilities for all device ports.

Restrictions

None

Example

This example shows auto-negotiation capabilities.

```
s# port show autonegotiation-capabilities all-ports
Port      Capability      Advertised      Received
et.2.1    10 baseT         10 baseT         10 baseT
          10 baseT HD      10 baseT HD
          10 baseT FD      10 baseT FD

          100 baseTX       100 baseTX       100 baseTX
          100 baseTX HD    100 baseTX HD
          100 baseTX FD    100 baseTX FD

et.2.2    10 baseT         10 baseT         10 baseT
          10 baseT HD      10 baseT HD      10 baseT HD
          10 baseT FD      10 baseT FD      10 baseT FD

          100 baseTX       100 baseTX       100 baseTX
          100 baseTX HD    100 baseTX HD    100 baseTX HD
          100 baseTX FD    100 baseTX FD    100 baseTX FD

et.2.3    10 baseT         10 baseT         10 baseT
          10 baseT HD      10 baseT HD
          10 baseT FD      10 baseT FD
          100 baseTX       100 baseTX       100 baseTX
```

port show bmon

Mode

Enable

Format

```
port show bmon
```

Description

The **`port show bmon`** command is to display storm protection information for the device.

Restrictions

None

Example

This example shows device storm protection information.

```
rs# port show bmon

Port bmon: Storm Protection rate_limit 1024  (packets-per-second)
  Storm Protection for broadcast       - enable
  Storm Protection for multicast       - disable
  Storm Protection for unknown-unicast - disable
```

port show description

Mode

Enable

Format

```
port show description <port-list> | all-ports
```

Description

The **port show description** command is to display the user defined description for device ports. The description is defined using the **port description** command.

The following table describes the command parameters.

Parameter	Value	Meaning
description	*<port-list>*	Specifies the ports to display the description
	all-ports	The all-ports keyword displays the description for all the device ports.

Restrictions

None

port show flowctl

Mode

Enable

Format

```
port show flowctl <port-list>|all-ports
```

Description

The **port show flowctl** command displays current and admin. flow-control status. Flow-control values are defined in the command **port set** command.

The following table describes the **port show flowctl** command parameters.

Parameter	Value	Meaning
flowctl	*<port-list>*	Specifies the ports to display the flow-control information.
	all-ports	The **all-ports** keyword displays the flow-control information for all ports.

Restrictions

None

Example

This example shows flow-control information for all ports.

```
rs# port show flowctl all-ports
                Current           Admin
Port            Flowcontrol       Flowcontrol
et.2.1           off               off
et.2.2           off               off
et.2.3           off               off
et.2.4           off               off
et.2.5           off               off
et.2.6           off               off
et.2.7           off               off
et.2.8           off               off
et.2.9           off               off
et.2.10          off               off
et.2.11          off               off
et.2.12          off               off
et.2.13          off               off
et.2.14          off               off
et.2.15          off               off
et.2.16          off               off
et.2.17          off               off
et.2.18          off               off
et.2.19          off               off
et.2.20          off               off
```

port show mirroring-status

Mode

Enable

Format

```
port show mirroring-status
```

Description

The **`port show mirroring-status`** command displays the port mirroring status information.

Restrictions

None

Example

This example shows port mirroring information.

```
rs# port show mirroring-status

Monitor port      Target port
et.2.17                et.2.2
```

port show port-status

Mode

Enable

Format

```
port show port-status <port-list>|all-ports
```

Description

The **port show port-status** command is to display port status information for ports.

The following table describes the command parameters.

Parameter	Value	Meaning
port-status	*<port-list >*	Specifies the ports for which to display status information
	all-ports	The **all-ports** keyword displays the description for all ports.

Restrictions

None

Example

This example shows the description for all ports.

```
rs# port show port-status all-ports
Flags: M - Mirroring enabled  S - SmartTRUNK port
                                          Negot-  Link      Admin
Port    Port Type         Duplex  Speed     iation  State     State   Flags
et.2.1  100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.2  100Mbit Ethernet  Full    100Mbits  Auto    Up         Up
et.2.3  100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.4  100Mbit Ethernet  Full    100Mbits  Auto    Up         Up
et.2.5  100Mbit Ethernet  Full    100Mbits  Auto    Up         Up
et.2.6  100Mbit Ethernet  Full    100Mbits  Auto    Up         Up
et.2.7  100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.8  100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.9  100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.10 100Mbit Ethernet  Full    100Mbits  Auto    Up         Up
et.2.11 100Mbit Ethernet  Full    100Mbits  Auto    Up         Up
et.2.12 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.13 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.14 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.15 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.16 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.17 100Mbit Ethernet  n/a     n/a       Auto    Down       Up      M
et.2.18 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
et.2.19 100Mbit Ethernet  n/a     n/a       Auto    Down       Up
```

port show stp-info

Mode

Enable

Format

```
port show stp-info <port-list>|all-ports
```

Description

The **port show stp-info** command is to display the Spanning Tree information for ports.

The following table describes the command parameters.

Parameter	Value	Meaning
Stp-info	*<port-list>*	Specifies the ports to display the Spanning Tree information..
	all-ports	The **all-ports** keyword displays the Spanning Tree information for all ports.

Restrictions

None

Example

This example shows ports Spanning Tree information.

```
rs# port show stp-info all-ports
Port      Priority  Cost   STP       State      Designated-Bridge  Port
----      --------  ----   ---       -----      -----------------  -----
et.2.1    128       19     Disabled  Disabled   32768:00028513bf20 128 1
et.2.2    128       19     Disabled  Disabled   32768:00028513bf20 128 2
et.2.3    128       19     Disabled  Disabled   32768:00028513bf20 128 3
et.2.4    128       19     Disabled  Disabled   32768:00028513bf20 128 4
et.2.5    128       19     Disabled  Disabled   32768:00028513bf20 128 5
et.2.6    128       19     Disabled  Disabled   32768:00028513bf20 128 6
et.2.7    128       19     Disabled  Disabled   32768:00028513bf20 128 7
et.2.8    128       19     Disabled  Disabled   32768:00028513bf20 128 8
et.2.9    128       19     Disabled  Disabled   32768:00028513bf20 128 9
et.2.10   128       19     Disabled  Disabled   32768:00028513bf20 128 10
et.2.11   128       19     Disabled  Disabled   32768:00028513bf20 128 11
et.2.12   128       19     Disabled  Disabled   32768:00028513bf20 128 12
et.2.13   128       19     Disabled  Disabled   32768:00028513bf20 128 13
et.2.14   128       19     Disabled  Disabled   32768:00028513bf20 128 14
et.2.15   128       19     Disabled  Disabled   32768:00028513bf20 128 15
et.2.16   128       19     Disabled  Disabled   32768:00028513bf20 128 16
et.2.17   128       19     Disabled  Disabled   32768:00028513bf20 128 17
```

port show vlan-info

Mode

Enable

Format

```
port show vlan-info <port-list>|all-ports
```

Description

The **port show vlan-info** command is to display device ports VLAN information.

The following table describes the command parameters.

Parameter	Value	Meaning
vlan-info	*<port-list>*	Specifies the ports to display VLAN information
	all-ports	The **all-ports** keyword displays the VLAN information for all the device ports.

Restrictions

None

Example

This example shows device port VLAN information.

```
rs# port show vlan-info all-ports
Port    Access Type Bridging VLANs
----    ----------- --------------
et.2.1  Access
et.2.2  Access
et.2.3  Access
et.2.4  Access
et.2.5  Access
et.2.6  Access
                    red
et.2.7  Access
                    red
et.2.8  Access
                    red
et.2.9  Access
                    default
et.2.10 Access
et.2.11 Access
                    default
et.2.12 Access
                    default
et.2.13 Access
                    default
```

25 PORT MIRRORING COMMANDS

The following table lists the **`port mirroring`** commands.

25.1 COMMAND SUMMARY

The sections following the table describe the command syntax for each command.

`port mirroring monitor-port <port num> target-port <port num>|target-profile <acl name>`
`no port mirroring monitor-port <port number> target-port <port number>|target-profile <acl name>`

port mirroring

Mode

Configure

Format

port mirroring monitor-port <port-num> target-port <port-num>|target-profile <acl name>

Description

The **port mirroring** command is to monitor via a single port the activity of a second port or the traffic specified by an ACL.

The following table describes the command parameters.

Parameter	Value	Meaning
Monitor-port	*<port num>*	The port used to monitor activity.
Target-port	*<port num>*	The port on which activity is monitored. Any single port can be specified.
target-profile	*<acl name>*	The ACL name that specifies the p traffic profile to monitor. The ACL must be a previously created IP ACL. The ACL may contain either **permit** or **deny** keywords. The **port mirroring** command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS.

Restrictions

Only one target port may be defined for a given device, and only one monitor port may be defined. Also, it is recommended that Gigabit ports are monitored through other Gigabit ports as there are speed-inconsistency-related problems monitoring a Gigabit port through a 10Base-T or 100Base-TX port.

no port mirroring

Mode

Configure

Format

```
no port mirroring monitor-port <port number> target-port <port number>|target-profile <acl name>
```

Description

The **no port mirroring** command is to stop monitoring a port.

The following table describes the command parameters.

Parameter	Value	Meaning
Monitor-port	*<port number>*	The port used to monitor activity.
Target-port	*<port number>*	The port on which activity is monitored. Any single port can be specified.
target-profile	*<acl name>*	The ACL name that specifies the traffic profile to monitor. The ACL must be a previously created IP ACL. The ACL may contain either **permit** or **deny** keywords. The **port mirroring** command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS.

Restrictions

None

26 QOS COMMANDS

The **qos** commands define and display Quality of Service (QoS) parameters. Use the command to classify Layer 2 and Layer traffic into the following priorities:

- Control
- High
- Medium
- Low

Assigning priorities to network traffic ensures that critical traffic reaches its destination even if the exit ports for the traffic are experiencing greater than maximum utilization. Use the **qos set l2** and **qos set ip** commands to assign priorities for Layer-2 and IP traffic respectively.

26.1 COMMAND SUMMARY

The following table lists the **qos** commands. The sections following the table describe the command syntax for each command.

qos apply priority-map <*string*> ports <*port list*>
qos create one-p-overwrite-map <*map*> <*num-list* >
qos create priority-map <*string*> <*num*> control | low | med | high
qos create tos-byte-overwrite-map <*map*> <*num-list*>
qos overwrite one-p-priority with tos-precedence|IEEE802dot1p-overwrite-map <*map*> list <*ifnames*>|<*port list*>
qos overwrite tos-byte-rewrite with tos-byte-overwrite-map <*map*> list <*port list*>|<*interface name*>
qos precedence ip [sip <*num*>] [dip <*num*>] [srcport <*num*>] [destport <*num*>] [tos <*num*>] [protocol <*num*>] [intf <*num*>]
qos priority-map off
qos set ip <*name*> <*priority*> [<*srcaddr/mask*> | any] [<*dstaddr/mask*> | any] [<*srcport*> | any] [<*dstport*> | any] [<*tos*> | any] [<*port list*> | <*interface-list*> | any] [<*protocol*> | any] [<*tos-mask*> | any] [<*tos-precedence-rewrite*> | any] [<*tos-rewrite*> | any]
qos set ip-acl <*string*> acl <*string*> priority low | medium | high | control list <*name/ipaddr*> tos-mask <*num*> tos-precedence-rewrite <*num*> tos-rewrite <*num*>
qos set l2 name <*name*> source-mac <*MACaddr*> *source-mac-mask* <*MACaddr*> dest-mac <*MACaddr*> dest-mac-mask <*MACaddr*> vlan <*vlan-num*> in-port-list <*port-list*> priority control | high | medium | low | <*trunk-priority*>

qos set queuing-policy weighted-fair port <*port list*> | all-ports
qos set weighted-fair control <*percentage*> high <*percentage*> medium <*percentage*> low <*percentage*> port <*port list*> | all-ports
qos show one-p-priority-overwrite-with-map <*map*> | all
qos show one-p-priority-overwrite-with-tos ports
qos show ip
qos show l2 all-destination all-flow ports <*port-list*> vlan <*vlanID*> source-mac <*MACaddr*> dest-mac <*MACaddr*> priority low | medium | high | control
qos show precedence
qos show priority-map <*string*> | all
qos show tos-byte-overwrite <*map*>|all
qos show wfq port <*port list*> | all-ports

qos apply priority-map

Mode

Configure

Format

```
qos apply priority-map <string> ports <port list>
```

Description

The **qos apply priority-map** command is to apply a previously defined priority map to a port or multiple ports. A priority map associates certain 802.1p tag values inside the frame to an internal priority queue. The **qos create priority-map** command is used to first create a priority map. By default, the device maps the number to the four internal priorities as follows:

- 0 or 1 = low
- 2 or 3 = medium
- 4 or 5 = high
- 6 or 7 = control.

The following table describes the command parameters.

Parameter	Value	Meaning
priority-map	*<string>*	Specifies the map name. Specify a string 25 characters or less.
port	*<port list>*	Specifies the port(s) to apply the priority map.

Restrictions

None

qos create one-p-overwrite-map

Mode

Configure

Format

```
qos create one-p-overwrite-map <map> <num-list >
```

Description

The **qos create one-p-overwrite-map** command is to map ToS precedence values in incoming packets to values written into the IEEE 802.1p priority fields in the same packets. For example, a packet with a ToS precedence value of ‚0™ can be mapped to an 802.1p value of ‚1™. Specify an 802.1p value for each of the ToS precedence values 0 through 7. After creating the map, use the **qos overwrite one-p-priority** command to overwrite the 802.1p fields according to the mapping.

The following table describes the command parameters.

Parameter	Value	Meaning
one-p-overwrite-map	<map>	This is the map name. Specify a string 25 characters or less.
	<num-list>	This is a list of eight values written into the 802.1p priority field. The range of each value is between 0 and 7. Specify a value for each of the eight possible ToS precedence values, starting with the value that maps to the ToS precedence ™0™. Use spaces between each number, for example, **1 3 4 2 6 7 5**. This example provides the following mapping: ToS Precedence Value 802.1p Priority ---------- ---------- 0 1 1 3 2 4 3 2 4 6 5 7 6 5 7 5

Restrictions

None

qos create priority-map

Mode

Configure

Format

```
qos create priority-map <string> <num> control | low | medium | high
```

Description

The **qos create priority-map** command is to map 802.1p tags from a frame to one of the four internal priority queue classes: **control**, **low**, **medium**, and **high**. Internal priority queue classes are used to prioritize flows during traffic congestion. The flows with the higher priority are given precedence over flow with a lower priority. The internal priority class **control** receives the highest precedence, while **low** receives the lowest precedence. With this command, a particular 802.1p priority tag can be mapped to a specific internal priority queue. By default, the device maps the number to the four internal priorities as follows:

- 0 or 3 = low
- 1 or 2 = medium
- 4 or 5 = high
- 6 or 7 = control.

The following table describes the command parameters.

Parameter	Value	Meaning
priority-map	<string>	Specifies the map name . Specify a string 25 characters or less.
	<num>	Specifies the 802.1p priority tag to be mapped. The range is between 0 and 7.
queue	control | high| medium | low	Specifies the internal priority queue. Specify the **control**, **high**, **medium**, or **low** queue.

Restrictions

None

qos create tos-byte-overwrite-map

Mode

Configure

Format

`qos create tos-byte-overwrite-map <map> <num-list>`

Description

The **`qos create tos-byte-overwrite-map`** command is to map IEEE 802.1p values in incoming packets to values written into the ToS byte in the same packets. For example, a packet with an 802.1p value of ‚0™ can be mapped to a ToS byte value of ‚100™. Specify a ToS byte value for each of the 802.1p values 0 through 7. After creating the map, use the **`qos overwrite tos-byte-rewrite`** command to rewrite the ToS byte according to the mapping.

The following table describes the command parameters.

Parameter	Value	Meaning
`tos-byte-overwrite-map`	*<map>*	This is the map name. Specify a string 25 characters or less.
	<num-list>	This is a list of eight values written into theToS field. The range of each value is between 0 and 255. Specify a ToS byte value for each of the eight possible 802.1p values, starting with the value that maps to 802.1p ‚0™. Use spaces between each number, for example, **`100 101 102 103 104 105 106 107`**. This example provides the following mapping: 802.1p Priority ToS Byte Value ---------- ---------- 0 100 1 101 2 102 3 103 4 104 5 105 6 106 7 107

Restrictions

None

qos overwrite one-p-priority

Mode

Configure

Format

```
qos overwrite one-p-priority with tos-precedence|IEEE802dot1p-overwrite-map <map> list
<ifnames>|<port list>
```

Description

The **qos overwrite one-p-priority** command is to overwrite the IEEE 802.1p value in incoming frames with either the ToS precedence value or with the corresponding value in an overwrite map created with the **qos create one-p-overwrite-map** command.

The following table describes the command parameters.

Parameter	Value	Meaning
tos-precedence		Writes the ToS precedence value in the packet into the 802.1p field. In Enable mode, use the **qos show one-p-priority-overwrite-with-tos** command to display the interfaces or ports where the 802.1p field is to be overwritten with the ToS precedence value.
IEEE802dot1P-overwrite-map	*<map>*	Overwrites the 802.1p field with the value according to an existing overwrite map. Specify in ***<map>*** the name of a map created with the **qos create one-p-overwrite-map** command. In Enable mode, use the **qos show one-p-priority-overwrite-with-map** command to display the interfaces or ports where the 802.1p field is to be overwritten with the values in the overwrite map.
list	*<ifnames>* | *<port list>*	Specifies the interfaces or ports where the 802.1p field in incoming packets are overwritten. If one or more ports are specified, the ports must be in VLANs on which L4 bridging is enabled. Separate multiple ports or interface names with commas.

Restrictions

None

qos overwrite tos-byte-rewrite

Mode

Configure

Format

`qos overwrite tos-byte-rewrite with tos-byte-overwrite-map <map> list <port list>|<interface name>`

Description

The **`qos overwrite tos-byte-rewrite`** command is to rewrite the whole ToS byte in incoming packets with the corresponding value in an overwrite map created with the **`qos create tos-byte-overwrite-map`** command.

The following table describes the command parameters.

Parameter	Value	Meaning
`tos-byte-overwrite-map`	*<map>*	Overwrites the whole ToS field with a value according to an existing overwrite map. Specify in ***<map>*** the name of a map created with the **`qos create tos-byte-overwrite-map`** command. In Enable mode, use the **`qos show tos-byte-overwrite`** command to display the interfaces or ports where the ToS field is overwritten with the values in the overwrite map.
`list`	*<port list>* | *<interface name>*	Specifies the interfaces or ports where the ToS field in incoming packets are overwritten. If one or more ports are specified, the ports must be in VLANs on which L4 bridging is enabled. Separate multiple ports or interface names with commas.

Restrictions

None

qos precedence ip

Mode

Configure

Format

```
qos precedence ip [sip <num>] [dip <num>] [srcport <num>] [destport <num>] [tos <num>]
[protocol <num>] [intf <num>]
```

Description

The **qos precedence ip** command is to set the QoS precedence for various flow fields in IP traffic. Set a precedence from 1 to 7 for the following IP fields:

- IP source address
- IP destination address
- Source TCP or UDP port
- Destination TCP or UDP port
- Type of Service (TOS) for the packet
- Protocol (TCP or UDP)
- Incoming interface

Precedence 1 is the highest priority. IP interfaces or flow fields within IP packets that have a precedence of 1 are given first priority. The default priorities are as follows:

- Destination port (1)
- Destination address (2)
- Source port (3)
- Source IP address (4)
- TOS (5)
- Interface (6)
- protocol (7).

The following table describes the command parameters.

Parameter	Value	Meaning
sip	<num>	Specifies the source address field precedence in IP flows. Specify a precedence from 1 to 7.
dip	<num>	Specifies the destination address field precedence in IP flows. Specify a precedence from 1 to 7.
srcport	<num>	Specifies the source port field precedence in IP flows. Specify a precedence from 1 to 7.
dstport	<num>	Specifies the port field precedence destination in IP flows. Specify a precedence from 1 to 7.
tos	<num>	Specifies the TOS field precedence in IP flows. Specify a precedence from 1 to 7.
protocol	<num>	Specifies the transport layer protocol name field precedence in the IP flows. Specify a precedence from 1 to 7.
intf	<num>	Specifies the IP interface precedence based on the interface name. Specify a precedence from 1 to 7.

Specify a precedence from 1 to 7.

Restrictions

None

qos priority-map off

Mode

Configure

Format

```
qos priority-map off
```

Description

The **qos priority-map off** command is to disable any priority maps applied on a port using the **qos apply priority-map** command. Maps set to off are still displayed by the command **qos show priority-map** in the default table. By default, the device maps the number to the four internal priorities as follows:

- 0 or 3 = Low
- 1 or 2 = Medium
- 4 or 5 = High
- 6 or 7 = Control

Restrictions

None

qos set ip

Mode

Configure

Format

```
qos set ip <name> <priority> [<srcaddr/mask> | any] [<dstaddr/mask> | any] [<srcport> | any]
[<dstport> | any] [<tos> | any] [<port list> | <interface-list> | any] [<protocol> | any]
[<tos-mask> | any] [<tos-precedence-rewrite> | any] [<tos-rewrite> | any]
```

Description

The **qos set ip** command sets the priority for an IP flow based on the following fields in the flow:

- Flow name
- Source IP address and network mask
- Destination IP address and network mask
- Source port
- Destination port
- TOS
- Layer 4 bridging port list or interface list
- Transport layer protocol (TCP or UDP)

Each field priority can be set for control, low, medium, or high. The default is low.

The following table describes the command parameters.

Parameter	Value	Meaning
ip	<name>	Specifies the IP flow name.
	<priority>	Specifies the priority being assigned to the flow parameters specified from the list. One of the following priorities can be specified: • control • high • medium • low
	control	Assigns control priority to the specified IP flow parameters. This is the highest priority.
	high	Assigns high priority to the specified IP flow parameters.
	medium	Assigns medium priority to the specified IP flow parameters.
	low	Assigns low priority to the specified IP flow parameters. This is the default.
	<srcaddr/mask> | any	Specifies the source IP address and network mask to assign a priority. The mask can be specified using the traditional IP address format, 255.255.0.0, or the CIDR format, /16. If **any** is specified instead of a network mask, the device assumes a wildcard *don't care* condition. If a mask is not specified, then the mask 255.255.255.255 is assumed. The mask connot be substituted with the **any** keyword. The keyword **any** is for the entire

	<srcaddr/mask> pair.

	<dstaddr/mask> | any	Specifies the destination IP address and network mask to assign a priority. The same requirements and restrictions for ***<srcaddr/mask>*** apply to ***<dstaddr/mask>***. If any is specified instead of a network mask, the device assumes a wildcard *don't care* condition. If a mask is not specified, then the device assumes a mask of 255.255.255.255. The **any** keyword is not a substitute for Mask. The keyword **any** is for the entire ***<dstaddr/mask>*** pair.
	<srcport> | any	Specifies the source TCP or UDP port to assign a priority. Specify a port number from 1 to 65535 or **any** to allow any value.
	<dstport> | any	Specifies the destination TCP or UDP port to assign a priority. Specify a port number from 1 to 65535 or **any** to allow any value.
	<tos> | any	Specifies the TOS to assign a priority. Specify a number from 0 to 255 or any to allow any value.
	<port list> |*<interface-list>* | any	Specifies one or more Layer 4 bridging ports or one or more IP interface names for which a priority is assigned. If a list is specified, delimit the interface names with commas. Specify **any** to allow any IP interface name.
	<protocol> | any	Specifies the transport layer protocol for which priority is assigned The possible values are as follows:
	tcp	Assigns the priority parameters to the TCP protocol.
	Udp	Assigns the priority parameters to the UDP protocol.
	any	Assigns the priority parameters to both the TCP and UDP protocols.
	<tos-mask>	Specifies the mask used for the TOS byte. Specify a number from 1 to 255 or **any** to specify any TOS value. The default is 30.
	<tos-precedence-rewrite>	Rewrites the TOS field precedence portion with a new value. Specify a number from 0-7 or **any** to specify any TOS value.
	<tos-rewrite>	Rewrites the TOS byte DSCP field with a new value. Specify a number from 0-63 or **any** to specify any TOS value.

Note If the TOS precedence rewrite is set to **any** and a value is specified for***<tos-rewrite>***, then the TOS field precedence portion field remains the same as in the packet, but the rest of the TOS field is rewritten. If both values are specified to ***<tos-precedence-rewrite>*** and ***<tos-rewrite>***, then the TOS field precedence portion is rewritten to the new ***<tos-precedence-rewrite>*** number and the rest of the TOS field is rewritten to the new ***<tos-rewrite>*** number.

Restrictions

None

qos set ip-acl

Mode

Configure

Format

```
qos set ip-acl <string> acl <string> priority low | medium | high||control list <name/ipaddr>
[tos-mask <num>] [tos-precedence-rewrite <num>] [tos-rewrite <num>]
```

Description

The **qos set ip-acl** command sets the priority for an IP flow based on a predefined ACL policy. This command is a shortcut for using the **qos set ip** command with a particular ACL policy. Since the ACL policy contains the following information, do not specify the information already inherent in the ACL policy.

- Flow name
- Source IP address and network mask
- Destination IP address and network mask
- Source port
- Destination port
- TOS
- Layer 4 bridging port list or interface list
- Transport layer protocol (TCP or UDP)

The following table describes the command parameters.

Parameter	Value	Meaning
ip-acl	*<string>*	Sets a priority for an IP flow using a predefined ACL. Specify a character string to identify the QoS profile.
acl	*<string>*	Specifies ACL(s) for matching IP flows.
		Specifies the 802.1Q priority value or a keyword that specifies the internal priority. Specify one of the following:
	high	High priority.
	medium	Medium priority.
	control	Control priority.
list	*<name/port_list>* | any	Interface name or port list for L2 bridging VLAN. Specify **any** to enable L2 bridging VLAN on all interfaces.
tos-mask	*<tos-mask>* | any	Specifies the mask used for the TOS byte. Specify a number from 1-255 or **any** to specify any TOS value. The default is 30.
tos-precedence-rewrite	*<tos-precedence-rewrite>* | any	Rewrites the TOS field precedence portion with a new value. Specify a number from 0 to 7 or **any** to specify any TOS value.
tos-rewrite	*<tos-rewrite>* | any	Rewrites the TOS byte DSCP field with a new value. Specify a number from 0 to 63 or **any** to specify any TOS value.

Note If **any** is set for the TOS precedence rewrite and a value is specified for ***<tos-rewrite>***, then the TOS field precedence portion remains the same as in the packet, but the rest of the TOS field is rewritten. If values are specified for both ***<tos-precedence-rewrite>*** and ***<tos-rewrite>***, then the TOS field precedence portion is rewritten to the new ***<tos-precedence-rewrite>*** number and the rest of the TOS field is rewritten to the new ***<tos-rewrite>*** number.

Restrictions

None

qos set l2

Mode

Configure

Format

```
qos set l2 name <name> source-mac <MACaddr> source-mac-mask <MACaddr> dest-mac <MACaddr>
dest-mac-mask <MACaddr> vlan <vlan-num> in-port-list <port-list> priority control | high |
medium | low | <trunk-priority>
```

Description

The **qos set l2** command sets QoS priority for Layer 2 flows. Set a priority for a flow based on the following fields in the flow:

- L2 flow name
- Source MAC address
- Destination MAC address
- VLAN ID
- Incoming port(s)

The priority can be set in one of the following ways:

• The flow is assigned a priority within the device. Specify a priority of control, low, medium, or high. The default is low.

• The flow is assigned a priority within the device and in addition, if the exit ports are VLAN trunk ports the flow is assigned an 802.1Q priority. In this case specify a number from 0 to 7. The device maps the number to the four internal priorities as follows:

- 0 = Low
- 1, 2 or 3 = Medium
- 4, 5 or 6 = High
- 7 = Control

The following table describes the command parameters.

Parameter	Value	Meaning
name	<name>	Specify the L2 flow name.
source-mac	<MACaddr> | any	This is the L2 source MAC address used to create a flow priority entry. Specify the MAC address in either of the following formats: xx:xx:xx:xx:xx:xx xxxxxx:xxxxxx Specify **any** to allow any MAC address as the L2 source MAC address.
source-mac-mask	<MACaddr>	Specify the source MAC mask address.
dest-mac	<MACaddr> | any	Specify the L2 destination MAC address used to create either a destination priority entry (without a source-mac defined) or a flow priority entry (with a source-mac defined.) Specify **any** to allow any MAC address as the L2 destination MAC address.
dest-mac-mask	<MACaddr>	Specify the destination MAC mask address.

vlan	vlan *<vlan-num>* | any	Specifies the VLAN number. Specify **any** to allow any VLAN.
in-port-list	*<port-list>*	Specify the ports to set priority for this flow. The priority applies when the L2 packet enters the device on one of the specified ports. The priority does not apply to exit ports.
Priority	control | high | medium | low | *<trunk-priority>*	This sets the priority for the flow. Specify one of the following priorities:
	control	Assigns control priority to the IP flow specified. This is the highest priority.
	high	Assigns high priority to the IP flow specified.
	medium	Assigns medium priority to the IP flow specified.
	low	Assigns low priority to the IP flow specified. This is the default.
	<trunk-priority>	Assigns an 802.1Q VLAN trunk priority when the exit port is a VLAN trunk port. The device maps the number to the four internal priorities as follows: • 0 = Low • 1, 2, or 3 = Medium • 4, 5,or 6 = High • 7 = Control

Restrictions

None

qos set queing-policy

Mode

Configure

Format

```
qos set queuing-policy weighted-fair port <port list> | all-ports
```

Description

The **`qos set queuing-policy`** command overrides the default queuing policy (strict priority) in favor of weighted-fair queuing on specific ports or on all ports. Only one type of queuing policy can be active at a time for a port.

Note Setting a queuing policy to one port automatically applies to all ports.

The following table describes the command parameters.

Parameter	Value	Meaning
`queuing-policy`	`weighted-fair`	Sets the queuing policy to weighted-fair.
`port`	*`<port list>`* | `all-ports`	Specify the Ethernet ports on which weighted-fair queuing apply. Use **`all-ports`** to apply weighted fair queuing to all ports.

Restrictions

None

qos set weighted-fair

Mode

Configure

Format

```
qos set weighted-fair control <percentage> high <percentage> medium <percentage> low
<percentage> port <port list> | all-ports
```

Description

The **qos set weighted-fair** command sets the bandwidth percentage allocated to the priority when the port uses weighted-fair queuing. The percentages apply to specific ports or to all ports. Make sure the combined percentage total for all four priorities equals 100.

Note Setting a weighted-fair policy to one port automatically applies to all ports.

The following table describes the command parameters.

Parameter	Value	Meaning
control	<*percentage*>	Specify the bandwidth percentage allocated to the control priority. The range for <*percentage*> is 1 to 97. The default is 25.
high	<*percentage*>	Specify the bandwidth percentage allocated to the high priority. The range for <*percentage*> is 1 to 97. The default is 25.
medium	<*percentage*>	Specify the bandwidth percentage allocated to the medium priority. The range for <*percentage*> is 1 to 97. The default is 25.
low	<*percentage*>	Specify the bandwidth percentage allocated to the low priority. The range for <*percentage*> is 1 to 97. The default is 25.
port	<*port list*> | all-ports	Specifies the Ethernet ports on which the defined percentages apply. Specify **all-ports** to apply the percentages to all ports.

Restrictions

The combined percentage total for all four QoS priorities equals 100.

qos show one-p-priority-overwrite-with-map

Mode

Enable

Format

```
qos show one-p-priority-overwrite-with-map <map> | all
```

Description

The **qos show one-p-priority-overwrite-with-map** command displays overwrite maps created with the **qos create one-p-overwrite-map** command and the interfaces or ports on which the maps are applied.

The following table describes the command parameters.

Parameter	Value	Meaning
one-p-priority-overwrite-with-map	<map>	Specify the name of a map to display.
	all	Specify **all** to display all the maps created.

Restrictions

None

qos show one-p-priority-overwrite-with-tos

Mode

Enable

Format

```
qos show one-p-priority-overwrite-with-tos ports
```

Description

The **qos show one-p-priority-overwrite-with-tos** command displays the interfaces or ports that were previously configured with 802.1p and now are configured with a new ToS value.

The following table describes the command parameters.

Parameter	Value	Meaning
one-p-priority-overwrite-with-tos		Specify whether interfaces or ports are displayed.
	ports	Specify **ports** to display all reconfigured ports.

Restrictions

None

qos show ip

Mode

Enable

Format

```
qos show ip
```

Description

The **`qos show ip`** command is to display QoS information for IP flows.

Restrictions

None

Example

The example shows the Profiles - i.e. to which queue each ACL is defined.

```
rs# qos show ip
Name:              profcon
Priority:          control
Interface:         int1
ACL:               aclcon
TosPrecedence:     any
TosByte:           any

Name:              profhi
Priority:          high
Interface:         int2
ACL:               aclhi
TosPrecedence:     any
TosByte:           any

Name:              proflw
Priority:          low
Interface:         int4
ACL:               acllw
TosPrecedence:     any
TosByte:           any
```

qos show l2

Mode

Enable

Format

```
qos show l2 all-destination all-flow ports <port-list> vlan <vlanID> source-mac <MACaddr>
dest-mac <MACaddr>
```

Description

The **qos show l2** command is to display QoS information for L2 flows. The display can be filtered according to the following parameters:

Format:

- Destinations
- Flows
- Ports
- VLANs
- Source MAC addresses
- Destination MAC addresses
- Priority

The following table describes the command parameters.

Parameter	Value	Meaning
l2	all-destination	Displays all the L2 destination priorities.
	all-flow	Displays all the L2 flow priorities.
ports	<port-list>	Displays L2 priority information for specific ports.
vlan	<vlanID>	Displays L2 priority information for specific VLANs.
source-mac	<MACaddr>	Displays L2 priority information for specific source MAC addresses.
dest-mac	<MACaddr>	Displays L2 priority information for specific destination MAC addresses.

Restrictions

None

qos show precedence

Mode

Enable

Format

```
qos show precedence ip
```

Description

The **`qos show precedence`** command is to display the precedence values for all fields in a flow:

- IP flows consist of the following fields:
- Destination Port
- Destination Address
- Source Port
- Source Ip Address
- Tos
- Interface
- Protocol

The following table describes the command parameters.

Parameter	Value	Meaning
`precedence`	`ip`	Displays the precedence values for IP flows.

Restrictions

None

Example

The following example shows the importance each parameter has in defining streams:

```
rs# qos show precedence ip

     Field           Precedence
     -----           ----------
     destport             1
     dip                  2
     srcport              3
     sip                  4
     tos                  5
     intf                 6
     protocol             7
```

qos show priority-map

Mode

Enable

Format

```
qos show priority-map <string> | all
```

Description

The **qos show priority-map** command displays the priority mapping configured on a port. The command displays how each 802.1p tag value is mapped to a specific internal priority queue. There are two types of displays:

- Applied – All mapped ports are displayed.
- Active – All active ports are displayed even if no active maps are created.

The following table describes the command parameters.

Parameter	Value	Meaning
priority-map	<string>	Specify the priority map name.
	all	Displays all priority maps.

Restrictions

None

Example

The example shows the 802.1p priority tag mapping to the 4 queues.

```
rs# qos show priority-map all
Map DEFAULT is applied on ports: et.2.(1-24),gi.1.(1-2),st.(1-6)
Map DEFAULT is active on ports: et.2.(1-24),gi.1.(1-2),st.(1-6)
 802.1p priority      internal priority
 ---------------      -----------------
  0                   low
  1                   low
  2                   medium
  3                   medium
  4                   high
  5                   high
  6                   control
  7                   control
```

qos show tos-byte-overwrite

Mode

Enable

Format

```
qos show tos-byte-overwrite <map>|all
```

Description

The **qos show tos-byte-overwrite** command displays overwrite maps created with the **qos create tos-byte-overwrite-map** command and the interfaces or ports on which the maps are applied.

The following table describes the command parameters.

Parameter	Value	Meaning
tos-byte-overwrite	<map>	Specify the overwrite map name to display.
all		Specify **all** to display all the maps created.

Restrictions

None

qos show wfq

Mode

Enable

Format

```
qos show wfq [port <port list> | all-ports]
```

Description

The **qos show wfq** command displays the bandwidth for each port allocated with weighted-fair queuing.

The following table describes the command parameters.

Parameter	Value	Meaning
port	<port list> | all-ports	Displays bandwidth allocated for each port. Specify a list of Ethernet or WAN ports. Specify **all-ports** to display bandwidth for all ports.

Restrictions

None

Example

This example shows the percentage each queue has, and whether it is set to priority or weighted fair queuing.

```
rs# qos show wfq port all-ports
Port     Q-Policy  Control  High  Medium  Low
----     --------  -------  ----  ------  ---
et.2.1   WFQ       50       25    15      10
et.2.2   WFQ       50       25    15      10
et.2.3   WFQ       50       25    15      10
et.2.4   WFQ       50       25    15      10
et.2.5   WFQ       50       25    15      10
et.2.6   WFQ       50       25    15      10
et.2.7   WFQ       50       25    15      10
et.2.8   WFQ       50       25    15      10
et.2.9   WFQ       50       25    15      10
et.2.10  WFQ       50       25    15      10
et.2.11  WFQ       50       25    15      10
et.2.12  WFQ       50       25    15      10
et.2.13  WFQ       50       25    15      10
et.2.14  WFQ       50       25    15      10
et.2.15  WFQ       50       25    15      10
et.2.16  WFQ       50       25    15      10
et.2.17  WFQ       50       25    15      10
et.2.18  WFQ       50       25    15      10
et.2.19  WFQ       50       25    15      10
et.2.20  WFQ       50       25    15      10
et.2.21  WFQ       50       25    15      10
```

27 RATE-LIMIT COMMANDS

The **rate-limit** commands are used to define rate limits and apply them to IP interfaces.

27.1 COMMAND SUMMARY

The following table lists the **rate-limit** commands. The sections following the table describe the command syntax.

rate-limit *<name>* port-level input port *<port list>* rate *<num>* [drop-packets | no-action | tos-rewrite *<num>*
rate-limit *<name>* port-level output port *<port list* | all-ports> rate *<num>* drop-packets
rate-limit show all
rate-limit show policy-type <portlevel-policies | all>
rate-limit show port-level [port <port list> | all-port] | [policy-name *<name>*]

rate-limit port-level input

Mode

Configure

Format

```
rate-limit <name> port-level input port <port list | all-ports> rate <num> [drop-packets | no-action | tos-rewrite <num>
```

Description

The **`rate-limit port-level input`** command is to specify a rate limiting policy on a per-port basis. This policy only affects incoming traffic on the port. The policy applies to a specific port and not an aggregation of flows.

The following table describes the command parameters.

Parameter	Value	Meaning
`rate-limit`	*<name>*	The rate limit name.
`port`	*<port list>*	Specify the ports on which to apply the rate-limiting policy.
	`all-ports`	Enables rate-limiting policy on all ports.
`rate`	*<num>*	Specify the rate limit, in bps, for the aggregation of flows. The range of ***<num>*** is 1000000 to 1000000000 inclusive.
`drop-packets`		This optional parameter specifies that if the rate-limit is exceeded, packets are dropped.
`no-action`		This optional parameter specifies that if the rate-limit is exceeded, no action is taken.
`tos-rewrite`	*<num>*	Specify this option to rewrite the ToS byte in the OSPF field when the rate limit is exceeded. The range for ***<num>*** is 0 to 63.

Restrictions

None

`

rate-limit port-level output

Mode

Configure

Format

```
rate-limit <name> port-level output port <port list | all-ports> rate <num> drop-packets
```

Description

The **rate-limit port-level output** command is to specify a policy for rate limiting on a per-port basis. This policy only affects outgoing traffic. The only exceed action available is **drop-packets**. This policy will only apply to a specific port and not an aggregation of flows.

The following table describes the command parameters.

Parameter	Value	Meaning
rate-limit	<name>	The rate limit name.
port	<port list>	Specify on which port to apply the rate-limiting policy.
	all-ports	Specify **all-ports** to enable rate limiting on all ports.
rate	<num>	The rate limit, in bps, for the flow. The range for <num> is 1000 to 1000000000.
drop-packets		This parameter specifies that if the rate-limit is exceeded, packets are dropped.

Restrictions

None

rate-limit show all

Mode

Enable

Format

```
rate-limit show all
```

Description

The **`rate-limit show policy-type`** command displays information about rate limiting policies.

The following table describes the command parameters.

Parameter	Value	Meaning
`show`	`all`	Displays information on all rate limiting policies.

Restrictions

None

rate-limit show policy-type

Mode

Enable

Format

```
rate-limit show policy-type <portlevel-policies | all>
```

Description

The **`rate-limit show policy-type`** command displays information about rate limiting policy types.

The following table describes the command parameters.

Parameter	Value	Meaning
`show`	`portlevel-policies`	Display all port level policies.
	`all`	Displays All policies.

Restrictions

None

rate-limit show port-level

Mode

Enable

Format

`rate-limit show port-level [port <port list> | all-port] | [policy-name <name>]`

The **`rate-limit show port-level`** command displays information about rate limiting port-level policies.

The following table describes the command parameters.

Parameter	Value	Meaning
`port`	`<port list>`	Show rate limiting parameters for a port. Requires a value of one of these types(Comma separated list allowed): • Gigabit - example: gi.5.1 • Ethernet - example: et.2.1
	`all-port`	On all ports.
`policy-name`	`<name>`	Display policy by name. The value must be one of the following types: • character string - A character string • [keyword] - One of the following keywords: - all – All policies

Restrictions

None

28 REBOOT COMMANDS

reboot

Mode

Enable

Format

```
reboot
```

Description

The **reboot** command reboots the device.

Restrictions

None

29 RIP COMMANDS

The Routing Information Protocol, Version 1 and Version 2 (RIPv1 and RIPv2), is the most commonly used interior gateway protocol. RIP selects the route with the lowest metric as the best route. The metric is a hop count representing the number of gateways through which data must pass in order to reach its destination. The longest path that RIP accepts is 15 hops. If the metric is greater than 15, a destination is considered unreachable and the device discards the route. RIP assumes that the best route is the one that uses the fewest gateways, that is, the shortest path. RIPv1 is described in RFC 1058 and RIPv2 is described in RFC 1723.

29.1 COMMAND SUMMARY

The following table lists the **rip** commands. The sections following the table describe the command syntax.

`rip add interface <interfacename-or-IPaddr>`
`rip set interface <interfacename-or-IPaddr> | All [receive-rip enable | disable] [send-rip enable | disable] [metric-in <num>] [version 1|version 2]`
`rip show <option-list>`
`rip start`
`rip stop`

rip add interface

Mode

Configure

Format

```
rip add interface <interfacename-or-IPaddr>
```

Description

By default, RIP is disabled on all interfaces. To enable RIP on an interface use the **`rip add interface`** command.

The following table describes the command parameters.

Parameter	Value	Meaning
`interface`		Informs the RIP process about the specified interfaces.
	`<interfacename-or-IPaddr>`	A list of interface names or IP addresses can be specified.

Restrictions

None

rip set interface

Mode

Configure

Format

```
rip set interface <interfacename-or-IPaddr> | All [receive-rip enable | disable] [send-rip
enable | disable] [metric-in <num>] [version 1|version 2]
```

Description

The **`rip set interface`** command lets is to set the following parameters for RIP interfaces:

- Whether the interface will accept RIP updates
- Whether the interface will send RIP updates
- The RIP version (RIP V1 or RIP V2)
- The packet type used for RIP V2 updates (broadcast or Multicast)
- The metric added to incoming RIP updates
- The metric added to outgoing RIP updates
- The key-chain for RIP update authentication
- The authentication method used for RIP updates (none, simple, or MD5)

The following table describes the command parameters.

Parameter	Value	Meaning
`interface`	*<interfacename-or-IPaddr>*	The interface names or IP addresses for which RIP parameters are set.
`all`		Specify the **`all`** keyword to set RIP parameters for all IP interfaces on the device.
`receive-rip`		This option affects RIP updates sent from trusted gateways.
	`enable`	RIP updates are received on the interface. _ Only updates from defined trusted gateways are accepted. The default is **`enable`**.
	`disable`	RIP updates are not received, including those sent from trusted gateways.
`send-rip`		Specifies whether the interface(s) can send RIP updates. This option does not affect the sending of updates to source gateways.
	`enable`	RIP updates are sent from this interface. The default is **`enable`**.
	`disable`	Specify that RIP updates are not sent from this interface.
`metric-in`	*<num>*	Specifies a metric that the interface adds to incoming RIP routes before adding them to the interface table. Specify a metric from 1 – 16. Use this option to make the device prefer RIP routes learned from the specified interfaces less than RIP routes from other interfaces. The default is 1.
`version 1`		Specifies that RIP version 1 is used on the interface(s).

`version 2`	Specifies that RIP version 2 is used on the interface(s).

Restrictions

Only RIP version 2 is supported.

rip show

Mode

Enable

Format

```
rip show <option-list>
```

Description

The **`rip show`** command displays RIP information.

The following table describes the command parameters.

Parameter	Value	Meaning
show	*<option-list>*	Specifies the RIP dump information to display.
	active-gateways	Displays active gateways running RIP.
	all	Displays all RIP tables.
	Export-policies	Displays RIP export policies.
	Globals	Displays RIP globals.
	Import-policies	Displays RIP import policies.
	Interface	Displays RIP interfaces.
	Interface-policies	Displays RIP interface policies.
	timers	Displays RIP timers.

Restrictions

None

Example

This example shows RIP globals.

```
rs# rip show globals

Rip Globals:
------------

Task Name          :RPTS
Send buffer size   :1472
Recv buffer size   :1472
Priority           :4
```

This example shows all RIP information.

```
rs# rip show all

Globals:
--------

Task Name          :RPTS
Send buffer size   :1472
Recv buffer size   :1472
Priority           :4

Timers:
-------

Timer                    State    Last     Next     Intvl Jitter Flags
                                  h:m:s    h:m:s    h:m:s  usec
-------------------------------------------------------------------------
RIP.0.0.0.0+520_Flash:
                         Inactive -        -        -     -      Inactive
RIP.0.0.0.0+520_Update:
                         Active                      30    10000000
RIP.0.0.0.0+520_Age:
                         Inactive -        -        -     -      Inactive
1. RIP Globals:
---------------

Task Name          : RPTS
Flags              : ON Broadcast Choose
Default metric     : 1
Default preference: 60
Auto Summarization: Enabled
Poison Reverse     : Enabled
Metric zero Routes: Rejected
Rip Loopback Count: 0


2. Targets:
   --------

Target 1.

================================================================
I/f Name              I/f Address     Source          Destination
--------              -----------     ------          -----------
int1                 1.1.1.1         1.1.1.1         1.255.255.255
Destination           Mask              Metric     Flags
-----------           ----              ------     -----
Target 2.

-----------           ----              ------     -----
Target 2.

================================================================
I/f Name              I/f Address     Source          Destination
--------              -----------     ------          -----------
int2                 2.1.1.1         2.1.1.1         2.255.255.255
Destination           Mask              Metric     Flags
-----------           ----              ------     -----
Target 3.

================================================================
I/f Name              I/f Address     Source          Destination
```

```
--------              -----------     ------          -----------
int3                3.1.1.1         3.1.1.1         3.255.255.255
Destination          Mask              Metric     Flags
-----------          ----              ------     -----
Target 4.

================================================================
I/f Name             I/f Address     Source          Destination
--------             -----------     ------          -----------
int4                4.1.1.1         4.1.1.1         4.255.255.255
Destination          Mask              Metric     Flags
-----------          ----              ------     -----
Target 5.

================================================================
I/f Name             I/f Address     Source          Destination
--------             -----------     ------          -----------
int5                5.1.1.1         5.1.1.1         5.255.255.255
Destination          Mask              Metric     Flags
-----------          ----              ------     -----
Target 6.

================================================================
I/f Name             I/f Address     Source          Destination
--------             -----------     ------          -----------
int10               10.1.1.1        10.1.1.1        10.255.255.255

3. RIP Gateways:
   -------------

4. RIP Interface Policy:
------------------------
Interface         : int1
RIP In            : YES
RIP Out           : YES

Interface         : int2
RIP In            : YES
RIP Out           : YES

Interface         : int3
RIP In            : YES
RIP Out           : YES

Interface         : int4
RIP In            : YES
RIP Out           : YES

Interface         : int5
RIP In            : YES
RIP Out           : YES

Interface         : int10
RIP In            : YES
RIP Out           : YES

5. Import policies from RIP to RIB:
   --------------------------------

6. Export policies from other protocols to RIP:
   ---------------------------------------------
```

This example shows RIP interface information.

```
rs# rip show interface int10

================================================================
I/f Name              I/f Address     Source          Destination
--------              -----------     ------          -----------
int10                10.1.1.1        10.1.1.1        10.255.255.255
Destination           Mask              Metric     Flags
-----------           ----              ------     -----
================================================================
```

This example shows RIP **`interface-p`** information.

```
rs# rip show interface-p

RIP Interface Policy:
---------------------
Interface         : int1
RIP In            : YES
RIP Out           : YES

Interface         : int2
RIP In            : YES
RIP Out           : YES

Interface         : int3
RIP In            : YES
RIP Out           : YES

Interface         : int4
RIP In            : YES
RIP Out           : YES

Interface         : int5
RIP In            : YES
RIP Out           : YES

Interface         : int10
RIP In            : YES
RIP Out           : YES
```

This example shows RIP **`timer`** information.

```
rs# rip show timers

Rip Timers:
-----------

Timer                   State    Last     Next     Intvl Jitter Flags
                                 h:m:s    h:m:s    h:m:s  usec
-------------------------------------------------------------------------
RIP.0.0.0.0+520_Flash:
                        Inactive -        -        -     -      Inactive
RIP.0.0.0.0+520_Update:
                        Active                      30    10000000
RIP.0.0.0.0+520_Age:
                        Inactive -        -        -     -      Inactive
```

rip start

Mode

Configure

Format

```
rip start
```

Description

The **rip start** command starts RIP on all IP interfaces for which RIP is enabled.

Note RIP is disabled by default.

Restrictions

None

rip stop

Mode

Configure

Format

```
rip stop
```

Description

The **`rip stop`** command stops RIP on all IP interfaces for which RIP is enabled.

Restrictions

None

30 RMON COMMANDS

The **rmon** commands are to display and set parameters for RMON statistics on a per-port basis. RMON information corresponds to RFCs 1757 and 2021.

30.1 COMMAND SUMMARY

The following table lists the **rmon** commands. The sections following the table describe the command syntax.

rmon alarm index <*index-number*> variable <*string*> [interval <*seconds*>] [falling-event-index <*num*>] [falling-threshold <*num*>] [owner <*string*>] [rising-event-index <*num*>] [rising-threshold <*num*>] [startup rising|falling|both] [status enable|disable]
rmon etherstats index <*index-number*> port <*port*> [owner <*string*>] [status enable|disable]
rmon event index <*index-number*> type none|log|trap|both [community <*string*>] [description <*string*>] [owner <*string*>] [status enable|disable]
rmon history index <*index-number*> port <*port*> [interval <*seconds*>] [owner <*string*>] [samples <*num*>] [status enable|disable]
rmon show alarm
rmon show etherstats <port-list>|all-ports
rmon show events
rmon show history <port-list>|all-ports

rmon alarm

Mode

Configure

Format

```
rmon alarm index <index-number> variable <string> [interval <seconds>] [falling-event-index <num>] [falling-threshold <num>] [owner <string>] [rising-event-index <num>] [rising-threshold <num>] [startup rising|falling|both] [status enable|disable]
```

Description

The **`rmon alarm`** command sets various RMON 1 Alarm control table parameters. The Alarm group takes periodic statistical samples and compares them with previously-configured thresholds. If a monitored variable crosses a threshold, an alarm is generated.

The following table describes the command parameters.

Parameter	Value	Meaning
index	*<index-number>*	A number that uniquely identifies an entry in the alarm table. The value must be between 1 and 65535, inclusive.
variable	*<string>*	Specifies the variable object identifier to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER may be sampled.
interval	*<seconds>*	Specifies the sampling interval in seconds when statistical variables samples are collected and compared to the rising and falling thresholds. The value must be between 1 and 2147483647, inclusive.
falling-event-index	*<num>*	The action taken as defined by the row with this index in the event table when a falling threshold is crossed. The value must be between 1 and 65535, inclusive.
falling-threshold	*<num>*	Specifies that the sample value must be less than or equal to the threshold to trigger an alarm. When the sample value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. The value must be between -2147483647 and 2147483647, inclusive.
owner	*<string>*	Specifies the alarm resource owner; for example, an IP address, machine name or person name.
rising-event-index	*<num>*	The action taken as defined by the row with this index in the event table when a rising threshold is crossed. The value must be between 1 and 65535, inclusive.
rising-threshold	*<num>*	Specifies that the sample value must be greater than or equal to the threshold to trigger an alarm. When the sample value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. The value must be between -2147483647 and 2147483647, inclusive.
startup	*<keyword>*	Specifies the condition for which the alarm is to be generated.
	rising	Causes an alarm to be generated if the sampled variable is greater than or equal to the rising threshold.
	falling	Causes an alarm to be generated if the sampled variable is less than or equal to the falling threshold.

Parameter	Value	Meaning
	both	Causes an alarm to be generated if the sampled variable is greater than or equal to the rising threshold or less than or equal to the falling threshold.
status	enable	Enables this alarm.
	disable	Disables this alarm.

Restrictions

None

rmon etherstats

Mode

Configure

Format

```
rmon etherstats index <index-number> port <port> [owner <string>] [status enable|disable]
```

Description

The **rmon show etherstats** command is used to display the Etherstats data. The Etherstats group contains port statistics. The **rmon etherstats** command sets various RMON 1 Etherstats control table parameters. If default tables are turned on for the Lite group, a entry is created in the Etherstats control table for each available port.

The following table describes the command parameters.

Parameter	Value	Meaning
index	<index-number>	Is a number between 1 and 65535 that uniquely identifies a row in the Etherstats control table.
port	<port>	Specifies the physical port from which to collect data.
owner	<string>	Specifies the event owner; for example, an IP address, machine name or persons name.
status	enable	Enables Etherstat. The default is enable.
	disable	Disables Etherstat.

Restrictions

None

rmon event

Mode

Configure

Format

```
rmon event index <index-number> type none|log|trap|both [community <string>] [description
<string>] [owner <string>] [status enable|disable]
```

Description

The **rmon show event** command is used to display the event data.

The Event group controls event generation and notification. The **rmon event** command sets various RMON 1 Event control table parameters.

The following table describes the command parameters.

Parameter	Value	Meaning
index	*<index-number>*	Is a number between 1 and 65535 that uniquely identifies an entry in the Event table.
type		Specifies what action is taken when the event occurs.
	none	No notification is sent for the event.
	log	An entry for the event is made in the log table for each event.
	trap	An SNMP trap is sent to one or more management stations for the event.
	both	Both an entry is made in the log table and an SNMP trap is sent to one or more management stations.
community	*<string>*	Specifies the SNMP community string sent with the trap. If an SNMP trap is sent, it goes to the SNMP community specified in this string.
description	*<string>*	Specifies a comment describing this event.
owner	*<string>*	Specifies the event owner; for example, an IP address, machine name or person name.
status	enable	Enables this event. The default is enable.
	disable	Disables this event.

Restrictions

None

rmon history

Mode

Configure

Format

```
rmon history index <index-number> port <port> [interval <seconds>] [owner <string>] [samples <num>] [status enable|disable]
```

Description

Use the **rmon show history** command to display the history data.

The RMON History group periodically records variable samples and stores them for later retrieval. The **rmon history** command is used to specify the port to collect data from, the number of samples, the sampling interval, and the owner. If default tables were turned on for the Lite group, an entry is created in the History control table for each available port.

The following table describes the command parameters.

Parameter	Value	Meaning
index	*<index-number>*	Is a number between 1 and 65535 that uniquely identifies an entry in the History table.
port	*<port>*	Specifies the port from which to collect data.
interval	*<seconds>*	Specifies the sampling interval in seconds. This value must be between 1 and 3600, inclusive. The default value is 1800.
owner	*<string>*	Specifies the history resource owner; for example, an IP address, machine name or persons name.
samples	*<num>*	Specifies the number of samples collected before wrapping counters. This value must be between 1 and 65535, inclusive. The default value is 50.
status	enable	Enables this history control row. The default is enable.
	disable	Disables this history control row.

Restrictions

None

rmon show alarm

Mode

Enable

Format

```
rmon show alarm
```

Description

The **rmon show alarms** command displays the RMON Alarm table.

Restrictions

This command is only available the Lite group is configured.

rmon show etherstats

Mode

Enable

Format

`rmon show etherstats <port-list>|all-ports`

Description

The **`rmon show etherstats`** command displays entries in the Ethernet table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Lite group.

The following table describes the command parameters.

Parameter	Value	Meaning
`etherstats`	*<port-list >*	The port(s) for which Ethernet statistics are displayed. Statistics are collected and displayed only for ports on which RMON is enabled with the **`rmon set ports`** command.
	`all-ports`	The keyword **`all-ports`** is used to show Ethernet statistics on all ports.

Restrictions

This command is only available the Lite group is configured.

rmon show events

Mode

Enable

Format

```
rmon show events
```

Description

The **rmon show events** command displays triggered events and triggered event logs.

Restrictions

None

rmon show history

Mode

Enable

Format

`rmon show history <port-list>|all-ports`

Description

The **`rmon show history`** command displays entries stored in the RMON History group.

The following table describes the command parameters.

Parameter	Value	Meaning
`history`	*`<port-list >`*	The port(s) for which the history information is displayed.
	`all-ports`	The keyword **`all-ports`** is used to show history information on all ports.

Restrictions

None

31 SAVE COMMANDS

save

Mode

Configure

Format

```
save active|startup
```

Description

The **save** command saves the configuration changes entered during the current CLI session.

The following table describes the command parameters.

Parameter	Value	Meaning
active		The **active** keyword activates uncommitted changes in the scratchpad. The device accumulates configuration commands in the scratchpad until they are activated or cleared (or reboot). When the changes are activated, the device runs the commands.
startup		The **startup** keyword saves the running system configuration in the Startup configuration file and re-instated by the server the next time the device is rebooted.

Restrictions

None

32 SERVICE COMMANDS

Use the **service** commands to create rate-limit services and to apply them to IP interfaces.

32.1 COMMAND SUMMARY

The following table lists the **service** commands. The sections following the table describe the command syntax.

service <*name*> apply rate-limit acl <*aclname*> {interface <*interface-name*> | all} | port <*port-number*>
service <*name*> apply rate-limit mf-classifier {interface <*interface-name*> | all}| port <*port-number*> [source-addr-mask <*srcaddr*>] [destination-addr-mask <*dstaddr*>] [source-port <*num*> | <*port*>] [destination-port <*num*> | <*port*>] [tos <*num*>] [tos-mask <*tosmask*>] [any]
service <*name*> create rate-limit aggregate rate <*rate*> [no-action | drop-packets | tos-rewrite <*num*>
service <*name*> create rate-limit per-flow rate <*rate*> [exceed-action <*action*>]
service show rate-limit aggregate <*name*> | all [show-applied]
service show rate-limit all [show-applied]
service show rate-limit per-flow <*name*> | all [show-applied]

service apply rate-limit acl

Mode

Configure

Format

```
service <name> apply rate-limit acl <aclname> {interface <interface-name> | all} | port
<port-number>
```

Description

The **`service apply rate limit`** command applies a previously-defined rate limit service to an interface or to a port. It also specifies the traffic profile, via the ACL, to which the rate limit service applies.

The following table describes the command parameters.

Parameter	Value	Meaning
`service`	*`<name>`*	Rate limit service name.
`acl`	*`<acl-name>`*	ACL Name to apply the rate limit service.
`interface`	*`<interface-name>`*	Specify to which interface the service is applied.
	`all`	Applies the service to all interfaces.
`port`	*`<port-number>`*	Specify the port to apply the service. Only ports in L2 bridging mode can be applied.

Restrictions

None

service apply rate-limit mf-classifier

Mode

Configure

Format

```
service <name> apply rate-limit mf-classifier {interface <interface-name> | all} | port
<port-number> [source-addr-mask <srcaddr>] [destination-addr-mask <dstaddr>] [source-port
<num> | <port>] [destination-port <num> | <port>] [tos <num>] [tos-mask <tosmask>} [any]
```

Description

The **`service apply rate-limit mf-classifier`** command applies a rate limit service to an interface or to a port. Instead of using an ACL to define a traffic profile, the various parameters in this command can be used to define the traffic profile for the rate limit service.

The following table describes the command parameters.

Parameter	Value	Meaning
service	<name>	Rate limit service name.
interface	<interface-name>	Specify to which interface the service is applied.
	all	Applies the service to all interfaces.
port	<port-number>	Specify the port to apply the service. Only ports in L2 bridging mode can be applied.
	<SrcAddr/Mask>	The flow source address and the filtering mask. If the source address is a network or subnet address, supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. Specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”)
	<DstAddr/Mask>	The flow destination address and the filtering mask. The same requirements and restrictions for <*SrcAddr/Mask*> apply to <*DstAddr/Mask*>.
source-port	<num>	Specify a port number. A keyword can also be entered.
	<port>	Enter a keyword that identifies the port. The ports of some popular services have been defined as keywords.
	dns	DNS port (53)
	finger	Finger port (79)
	ftp-cmd	FTP command port (21)
	ftp-data	FTP data port (20)
	http	HTTP (WWW) port (80)
	https	HTTP-Secure (WWW) port (443)

	`imap3`	IMAP3 port (220)
	`imap4`	IMAP4 port (143)
	`lpr`	lpr port (515)
	`nfs`	`nfs` NFS port (2049)
	`nntp`	NNTP port (119)
	`ntp`	NTP port (123)
	`pop3`	POP3 port (110)
	`portmapper`	Portmapper port (111)
	`rexec`	R-Exec port (512)
	`rlogin`	R-Login port (513)
	`rshell`	R-Shell port (514)
	`snmp`	SNMP port (161)
	`smtp`	SMTP port (25)
	`telnet`	Telnet port (23)
	`tftp`	TFTP port (69)
	`x11`	X11 port (6000)
`destination-port`		Specify the rate-limited traffic destination port. The requirements, restrictions and possible values for this parameter are the same as the **`source-port`** parameter.
`tos`	*<tos>*	IP TOS (Type of Service) value. Specify a TOS value from 0 – 255.
`tos-mask`	*<tos-mask>*	Mask value used for the TOS byte. Specify a mask value from 0– 255. Default is 30. Specify **`any`** for any TOS value.
	`any`	Specify **`any`** for any ToS value.

Restrictions

None

service create rate-limit aggregate

Mode

Configure

Format

```
service <name> create rate-limit aggregate rate <rate> [no-action | drop-packets | tos-rewrite <num>]
```

Description

The **service create rate-limit aggregate** command specifies the rate limiting service for flows aggregation. This service affects the entire aggregation and not just individual flows.

The following table describes the command parameters.

Parameter	Value	Meaning
service	<name>	Rate limit service name.
rate	<rate>	The rate limit, in bits per second (bps), for flow aggregation. Enter a value between 100000000 to 1000000000, inclusive.
no-action		Specifies that no action is taken when the rate limit is exceeded.
drop-packets		Specifies that packets are dropped when the rate limit is exceeded.
tos-rewrite	<num>	Specifies that if the rate limit is exceeded, the ToS byte in the DSCP field is rewritten. The range of ***<num>*** is 0 to 63.

Restrictions

None

service create rate-limit per-flow

Mode

Configure

Format

```
service <name> create rate-limit per-flow rate <rate> [exceed-action <action>]
```

Description

The **`service create rate-limit per-flow`** command creates a rate limit service that limits an individual flow to the specified rate.

The following table describes the command parameters.

Parameter	Value	Meaning
`service`	*<name>*	Rate limit service name.
`rate`	*<rate>*	The rate limit, in bits per second (bps), for flow aggregation. For Fast Ethernet (FE) enter a value between 1000000 to 1000000000, inclusive. For Giga enter a value between 8000000 to 1000000000, inclusive.
`exceed-action`	*<action>*	The action taken if the rate limit is exceeded.
	`drop-packets`	Drop the packets.

Restrictions

None

service show rate-limit aggregate

Mode

Enable

Format

```
service show rate-limit aggregate <name> | all [show-applied]
```

Description

The **service show rate-limit aggregate** command displays the specified aggregate rate limit service(s).

The following table describes the command parameters.

Parameter	Value	Meaning
aggregate	<name>	Aggregate rate limit service name.
	all	Specify **all** to display all aggregate rate limit services.
show-applied		Displays where the service is applied.

Restrictions

None

service show rate-limit all

Mode

Enable

Format

```
service show rate-limit all [show-applied]
```

Description

The **`service show rate-limit all`** command displays all rate limit services.

The following table describes the command parameters.

Parameter	Value	Meaning
`show-applied`		Displays where the service is applied.

Restrictions

None

service show rate-limit per-flow

Mode

Enable

Format

```
service show rate-limit per-flow <name> | all [show-applied]
```

Description

The **service show rate-limit per-flow** command displays the specified per-flow rate limit service(s).

The following table describes the command parameters.

Parameter	Value	Meaning
per-flow	<name>	Per-flow rate limit service name.
	all	Specify **all** to display all aggregate rate limit services.
show-applied		Displays where the service is applied.

Restrictions

None

33 SHOW COMMANDS

show

Mode

Configure

Format

```
show running-config | startup-config
```

Description

The **show** command displays the system configuration currently running or the configuration the device starts up when the device is rebooted. In the **running-config** display each CLI command is preceded with a number. This number can be used with the **negate** command to negate one or more commands. If the character **E** (for Error) immediately follows the command number, it means the command did not execute successfully due to an earlier error condition. To get rid of the command in error, either negate it or fix the original error condition.

There are two modes for the **show** command: **running-config**, and **startup-config**. Specifying **running-config** shows the configuration currently active on the router. Specifying **startup-config** shows the configuration applied at the next bootup. One of these two modes must be selected as a parameter for the show command.

When viewing the active configuration file, the CLI displays the configuration file command lines with the following possible annotations:

- Commands without errors are displayed without any annotation.
- Commands with errors are annotated with an “E”.
- If an applied command is annotated with a “P” it can be expanded on additional interfaces. For example if STP is enabled on all ports in the current system, but there is only one current port, then whenever a port is added, it automatically is configured for STP.

  If a potentially partial command, which is configured to include all ports, becomes only partially activated, the status automatically changes to “P”.

Note Commands with no annotation or annotated with a “P:” are not in error.

The following table describes the command parameters.

Parameter	Value	Meaning
running-config		Specify this parameter to show the configuration currently active on the router.
startup-config		Specify this parameter to show the configuration applied at the next bootup.

Restrictions

None

Example

This example shows the configuration currently active on the router.

```
rs# show running-config
Running system configuration:
 1 : interface create ip reshet address-netmask
176.243.37.87/255.255.0.0 port e
t.2.4
 2 : interface create ip rr address-netmask 80.1.1.1 port et.2.23
 3 : interface create ip hamesh address-netmask 90.1.1.1 port et.2.5
 4 : interface create ip rri address-netmask 70.1.1.1 port et.2.6
 5 : interface create ip qa address-netmask 16.1.1.3 port et.2.2
 6 : interface create ip giga address-netmask 100.1.1.1/8 port gi.1.2
 7 : interface create ip re address-netmask 60.1.1.1/8 port et.2.22
 8 : interface create ip wa address-netmask 40.1.1.1 port et.2.10
 9 : interface create ip fs address-netmask 95.1.1.1 port et.2.11
     !
10 : ip add route 176.243.0.0/16 gateway 176.243.1.1
11 : ip add route default gateway 176.243.1.1
     !
12 : port mirroring monitor-port et.2.17 target-port et.2.2
     !
13 : system set location YYY
14 : system set location rs
15 : system set location none
16 : system set location Planet_Earth
17 : system set name rs
     !
18 : snmp set community public privilege read-write
```

This example shows the configuration applied at the next bootup.

```
rs# show startup-config
!
 ! Startup configuration for the next system reboot
interface create ip reshet address-netmask 176.243.37.87/255.255.0.0
port et.2.4
interface create ip rr address-netmask 80.1.1.1 port et.2.23
interface create ip hamesh address-netmask 90.1.1.1 port et.2.5
interface create ip rri address-netmask 70.1.1.1 port et.2.6
interface create ip qa address-netmask 16.1.1.3 port et.2.2
interface create ip giga address-netmask 100.1.1.1/8 port gi.1.2
interface create ip re address-netmask 60.1.1.1/8 port et.2.22
interface create ip wa address-netmask 40.1.1.1 port et.2.10
interface create ip fs address-netmask 95.1.1.1 port et.2.11
ip add route 176.243.0.0/16 gateway 176.243.1.1
ip add route default gateway 176.243.1.1
port mirroring monitor-port et.2.17 target-port et.2.2
```

```
system set location YYY
system set location rs
system set location none
system set location Planet_Earth
system set name rs
snmp set community public privilege read-write
```

34 SMARTTRUNK COMMANDS

The **smarttrunk** commands are to display and set parameters for SmartTRUNK ports. SmartTRUNK ports are groups of ports logically combined to increase throughput and provide link redundancy.

34.1 COMMAND SUMMARY

The following table lists the smarttrunk commands. The sections following the table describe the command syntax.

smarttrunk add ports <*port list*> to <smarttrun*k*>
smarttrunk create <smarttrun*k*> protocol no-protocol
smarttrunk set load-balancing <*smarttrunk*> <bridging | routing>[layer <*num*>][UsedAddresses <notApplied | dstAddr | srcAddr | dstAndSrcAddr | vlanId | ethType>]
smarttrunk show connections <smarttrunk *list*>|all-smarttrunks
smarttrunk show load-balancing <*smarttrunk*>|all-smarttrunks
smarttrunk show protocol-state <smarttrunk *list*>|all-smarttrunks
smarttrunk show trunks <smarttrunk *list*>|all-smarttrunks

smarttrunk add ports

Mode

Configure

Format

`smarttrunk add ports <port list> to <smarttrunk>`

Description

The smarttrunk **`add ports`** command is to add the ports specified in <*port list*> to a SmartTRUNK. The ports in the SmartTRUNK must be set to full duplex and auto-negotiation set to off.

The following table describes the command parameters.

Parameter	Value	Meaning
`ports`	`<port list>`	One or more ports to be added to an existing SmartTRUNK. All the ports in the SmartTRUNK must be connected to the same destination.
	`<smarttrunk>`	The name of an existing SmartTRUNK.

Restrictions

Ports added to a SmartTRUNK must:

- Be set to full duplex.
- There is not a L3 interface defined on the port.
- The port does not belong to any VLAN (it can belongs to the default VLAN).
- The port does not belong to any trunk.
- The port is not a copy port.
- The port is not in auto-negotiation mode.
- The port is in FULL DUPLEX mode.
- If the port is not the first port of the giving trunk it has the same speed as the other ports belonging to the trunk.
- If QoS is not defined on the port.
- If the port is not GVRP enabled.

smarttrunk create

Mode

Configure

Format

```
smarttrunk create <smarttrunk> protocol no-protocol
```

Description

The **smarttrunk create** command is used to create a SmartTRUNK. Once a SmartTRUNK is created, add physical ports to it with the smarttrunk **smarttrunk add ports** command.

SmartTRUNKs supports the 803.ad standard Link Aggregation Control Protocol (LACP), which aggregates links into Link Aggregation Groups (LAGs) and assigns them to an Aggregator (SmartTRUNK).

If a SmartTRUNK is connected to a device that does not support LACP, no control protocol is used. In this case, specify the **no-protocol** keyword in the **smarttrunk create** command.

The following table describes the command parameters.

Parameter	Value	Meaning
create	*<smarttrunk>*	The SmartTRUNK name. The SmartTRUNK name must be in the form **st.**x; for example, **st.**1.
protocol		Specifies the control protocol to be used.
	no-protocol	Specifies that no control protocol be used. Use this keyword if the SmartTRUNK is connected to a device that does not support LACP.

Restrictions

None

smarttrunk set load-balancing

Mode

Configure

Format

```
smarttrunk set load-balancing <smarttrunk> <bridging | routing>[layer <num>][UsedAddresses
<notApplied | dstAddr | srcAddr | dstAndSrcAddr | vlanId | ethType>]
```

Description

The **`smarttrunk set load-balancing`** command is to set a balancing criterion used for the corresponding Trunk.

The following table describes the command parameters.

Parameter	Value	Meaning
`load-balancing`	*`<smarttrunk>`*	The name of one or more SmartTRUNKs.
	`bridging`	Specifies load-balancing for a SmartTRUNK configured as part of a bridge.
	`routing`	Specifies load-balancing for a SmartTRUNK configured as part of a router.
`layer`	*`<num>`*	Specifies the network layer number.
`UsedAddresses`		Specifies to which addresses to configure load-balancing.
	`notApplied`	Specifies that no specific address is defined.
	`dstAddr`	Specifies a destination address to apply load-balancing.
	`srcAddr`	Specifies a source address to apply load-balancing.
	`dstAndSrcAddr`	Specifies a destination and source address to apply load-balancing.
	`vlanId`	Specifies a VLAN to apply load-balancing.
	`ethType`	Specifies an Ethernet type apply load-balancing.

Restrictions

There are restrictions for apply to certain layer/parameter combinations. The following table illustrates these combinations.

Table 34-1 Smarttrunk set load-balancing restrictions

	Bridging	Routing
Layer 2	vlanId and ethType are restricted	Restricted
Layer 3	vlanId and ethType are restricted	Only dstAddr is permitted ethType, srcAddr and dstAndSrcAddr are restricted
Layer 4	Restricted	Restricted

smarttrunk show connections

Mode

Enable

Format

```
smarttrunk show connections < smarttrunk list >|all-smarttrunks
```

Description

The **smarttrunk show connections** command displays information about the SmartTRUNK connection, including the remote switch MAC address, and port number of each remote port. Connection information is reported only if the Hunt Group protocol is enabled for the SmartTRUNK.

The following table describes the command parameters.

Parameter	Value	Meaning
connections	*<smarttrunk list>*	The name of one or more SmartTRUNKs.
	all-smarttrunks	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None

smarttrunk show load-balancing

Mode

Enable

Format

```
smarttrunk show load-balancing <smarttrunk> | all smarttrunks
```

Description

The **`smarttrunk show load-balancing`** command is to display SmartTRUNKS configured for load-balancing.

The following table describes the command parameters.

Parameter	Value	Meaning
`load-balancing`	*`<smarttrunk>`*	The name of one or more SmartTRUNKs to display.
	`all smarttrunks`	Specifies that all SmartTRUNKs are displayed.

Restrictions

None

smarttrunk show protocol-state

Mode

Enable

Format

```
smarttrunk show protocol-state < smarttrunk list >|all-smarttrunks
```

Description

The smarttrunk **`show protocol-state`** command displays information about the control protocol on a SmartTRUNK and the state of its ports.

The following table describes the command parameters.

Parameter	Value	Meaning
`protocol-state`	*`<smarttrunk list>`*	The name of one or more SmartTRUNKs.
	`all-smarttrunks`	Specifies that the command be applied to all SmartTRUNKs.

Restrictions

None

smarttrunk show trunks

Mode

Enable

Format

```
smarttrunk show trunks
```

Description

The **`show trunks`** command displays information about all SmartTRUNKs, including active and inactive ports, and the control protocol used.

Restrictions

None

35 SNMP COMMANDS

The Simple Network Management Protocol (SNMP) is an application layer protocol used to monitor and manage TCP/IP-based networks. The device supports all three versions: SNMPv1, SNMPv2c, and SNMPv3. Use the **snmp** commands to set and show SNMP parameters.

35.1 COMMAND SUMMARY

The following table lists the **snmp** commands. The sections following the table describe the command syntax.

snmp set community <*community-name*> privilege read|read-write
snmp set target <*IP-addr*> community <*community-name*> [owner <*name*>] [port <*number*>] [status enable|disable]
snmp show all | community |trap

snmp set community

Mode

Configure

Format

`snmp set community <community-name> privilege read|read-write`

Description

The **`snmp set community`** command sets a community string for SNMP access to the device. For SNMP management to access the device, a community string already set on the switch must be supplied. This command also sets the level of access to the device as read-only or read-write. Read-only communities allow SNMP GETs but not SNMP SETs. Read-write access communities allow both SNMP GETs and SNMP SETs.

The following table describes the command parameters.

Parameter	Value	Meaning
`community`	*`<community-string>`*	Character string for the community string.
`privilege`		Specifies the access level.
	`read`	Allows SNMP GETs but not SNMP SETs.
	`read-write`	Allows SNMP GETs and not SNMP SETs.

Restrictions

None

snmp set target

Mode

Configure

Format

```
snmp set target <IP-addr> community <community-name> [owner <name>] [port <number>] [status
enable|disable]
```

Description

The **`snmp set target`** command specifies the target server IP address the device to sends SNMP traps. Trap targets are enabled by default but the status argument is to disable or re-enable a target.

Note In general, community strings sent with traps do not have read-write privileges.

The following table describes the command parameters.

Parameter	Value	Meaning
`target`	*<IP-addr>*	The management station IP address from which to access the traps. The target IP address must be locally attached to the device. Cold start traps might not reach their destination if the target requires dynamic route table entries to be forwarded correctly. The device retries every minute up to four minutes on the cold-start trap.
`community`	*<community-name>*	The SNMP community name for the set trap target.
`owner`	*<name>*	The administrative owner for this trap destination. The default is monitor.
`port`	*<number>*	The UDP port to send the trap. Specify a value between 0-65535. The default is UDP port 162.
`status`	`enable`	Re-enables the target.
	`disable`	Disables the target.

Restrictions

None

snmp show community

Mode

Enable

Format

```
snmp show all | community |trap
```

Description

The **`snmp show community`** command displays the community strings set on the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`all`		Displays all SNMP information (equivalent to specifying all the other keywords).
`community`		Displays the device community string.
`trap`		Displays the trap target server IP address.

Restrictions

None

36 STATISTICS COMMANDS

The **statistics** commands are to display statistics for various features. Some statistics can be cleared using the command.

36.1 COMMAND SUMMARY

The following table lists the **statistics** commands. The sections following the table describe the command syntax.

statistics clear <statistic-type> <port-list>
statistics show arp <*string*>|all
statistics show icmp
statistics show ip
statistics show port-errors <port/SmartTRUNK-list>|all-ports
statistics show port-packets <port-list>|all-ports
statistics show port-stats <port/SmartTRUNK-list>|all-ports
statistics show tcp
statistics show udp

statistics clear

Mode

Enable

Format

```
statistics clear <statistic-type> <port-list>
```

Description

The **`statistics clear`** command clears port statistics, error statistics, IP, or ICMP statistics. When the statistics are cleared, the device sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

The following table describes the command parameters.

Parameter	Value	Meaning
`clear`	*`<statistic-type>`*	Type of statistics to clear.
	`icmp`	Clears all ICMP statistics for the specified port.
	`port-errors`	Clears all error statistics for the specified port.
	`port-packets`	Clears all packet statistics for the specified port.
	`port-stats`	Clears all normal (non-error) statistics for the specified port.
	`ip`	Clears all IP statistics for the specified port.
	`tcp`	Clears all TCP statistics for the specified port.
	`udp`	Clears all UDP statistics for the specified port.

Restrictions

None

statistics show arp

Mode

Enable

Format

```
statistics show arp <string>|all
```

Description

The **statistics show arp** command is to display Address Resolution Protocol (ARP) statistics.

The following table describes the command parameters.

Parameter	Value	Meaning
arp	*<string>*	Specifies the interface name.
	all	Specify **all** to display ARP statistics for all interfaces.

Restrictions

None

Example

This example shows all ARP statistics.

```
rs# statistics show arp all
  0  requests sent
  0  replies sent
  0  proxy replies sent
```

statistics show icmp

Mode

Enable

Format

```
statistics show icmp
```

Description

The **`statistics show icmp`** command is to display Internet Control Message protocol (ICMP) statistics.

Restrictions

None

Example

This example shows ICMP statistics.

```
rs# statistics show icmp
icmp:
         0 messages with smaller than minimum length
         0 messages with bad checksums
         0 messages with bad length
       370 message responses generated

Message Breakdown By Type:

--------------|--------------------|--------------------|
Message type  |   Input messages   |   Output messages  |
--------------|--------------------|--------------------|
echo reply    |          1         |          0         |
echo request  |          0         |          1         |
--------------|--------------------|--------------------|
```

statistics show ip

Mode

Enable

Format

```
statistics show ip
```

Description

The **`statistics show ip`** command is to display Internet Protocol (IP) statistics.

Restrictions

None

Example

This example shows IP statistics.

```
rs# statistics show ip
ip:
      5499 total packets received
        50 input packets discarded due to errors in their IP headers
         0 input packets discarded due to an invalid IP address
       757 input packets that this entity was not their final IP
destination
         0 packets for unsupported/unsupported protocol
         0 packets dropped due to no bufs, etc.
     10947 input packets successfully delivered to IP user-protocols
      4663 packets with local IP user-protocols
         0 output packets discarded
         0 output packets discarded due to no route
         0 fragments received
         0 packets re-assembled ok
         0 failures detected by the IP re-assembly algorithm
         0 packets that have been successfully fragmented
         0 packets discarded because they could not be fragmented
         0 fragments created
```

statistics show port-errors

Mode

Enable

Format

`statistics show port-errors <port/SmartTRUNK-list>|all-ports`

Description

The **`statistics show port-errors`** command is to display port error statistics.

The following table describes the command parameters.

Parameter	Value	Meaning
`port-errors`	*`<port/SmartTRUNK-list>`*	Specifies the port.
	`all-ports`	Specify **`all-ports`** to display port error statistics for all physical and logical ports.

Restrictions

None

Example

This example shows port error statistics.

```
rs# statistics show port-errors et.2.1

Port: et.2.1
-----
Error Stats                                Error Stats
-----------                                -----------
CRC errors                        0        Carrier sense error
0
Single collision (tx OK)          0        Many collisions
0
Many collisions (drop)            0        Late collisions
0
Long frames >1518                 0
Alignment errors                  0
Deferred transmissions            0
Internal frame tx error           0        Internal frame rx error
0
Error stats cleared  * Never Cleared *
```

statistics show port-packets

Mode

Enable

Format

```
statistics show port-packets <port-list>|all-ports
```

Description

The **statistics show port-packets** command is to display port packet statistics.

The following table describes the command parameters.

Parameter	Value	Meaning
port-packets	*<port-list>*	Specifies the port.
	all-ports	Specify **all-ports** to display port packet statistics for all physical and logical ports.

Restrictions

None

Example

This example shows a port packet statistics.

```
rs# statistics show port-packets et.2.3

The following ports are rmon etherstats disabled and should be enabled
to see statistics:

 et.2.3
```

This example shows a all port packet statistics

```
rs# statistics show port-packets all-ports

The follwing ports are rmon etherstats disabled and should be enabled to
see statistics:

 et.2.1 et.2.2 et.2.3 et.2.4 et.2.5 et.2.6 et.2.7 et.2.8 et.2.9et.2.10
et.2.11et.2.12et.2.13et.2.14et.2.15et.2.16et.2.17et.2.18et.2.19et.2.20
et.2.21et.2.22et.2.23et.2.24 gi.1.1 gi.1.2   st.1   st.2   st.3   st.4
   st.5   st.6
```

statistics show port-stats

Mode

Enable

Format

`statistics show port-stats <port/SmartTRUNK-list>|all-ports`

Description

The **`statistics show port-stats`** command is to display normal (non-error) port statistics.

The following table describes the command parameters.

Parameter	Value	Meaning
`port-stats`	*`<port/SmartTRUNK-list>`*	Specifies the port.
	`all-ports`	Specify **`all-ports`** to display port statistics for all physical and logical ports.

Restrictions

None

statistics show tcp

Mode

Enable

Format

```
statistics show tcp
```

Description

The **statistics show tcp** command is to display Transmission Control Protocol (TCP) statistics.

Restrictions

None

Example

This example shows TCP statistics.

```
rs# statistics show tcp
tcp:
          0 Active open connections
         11 Passive open connections
          0 Connections were closed before established
          9 Connections were reset after establish
          1 Connections currently established
       5311 Received packets
       4778 Sent packets
          6 Error packets
          9 Reset packet were sent
```

statistics show udp

Mode

Enable

Format

```
statistics show udp
```

Description

The **`statistics show udp`** command is to displays User Datagram Protocol (UDP) statistics.

Restrictions

None

Example

This example shows UDP statistics.

```
rs# statistics show udp
udp:
       298 datagrams received
      5239 datagrams dropped due to no socket
         0 datagrams errors
         0 datagrams output
```

37 STP COMMANDS

The **stp** commands are to display and change settings for the default Spanning Tree.

37.1 COMMAND SUMMARY

The following table lists the **stp** commands. The **stp** command is to display and change settings for the default Spanning Tree. The sections following the table describe the command syntax.

stp enable port <*port-list*>|all-ports
no stp enable port <*port-list*>|all-ports
stp filter-bpdu <*port-list*>
stp set bridging [forward-delay <*num*>] [hello-time <*num*>] [max-age <*num*>] [priority <*num*>] [damp-monitor-time <*num*>] [damp-bpdu-count <*num*>] >
stp set port <*port-list*> [[priority <*num*>[[port-cost <*num*>] [dampening enable|disable]]
stp show bridging-info
stp show dampening-info
stp show protocol-version

stp enable port

Mode

Configure

Format

`stp enable port <port-list>|all-ports`

Description

The **`stp enable port`** command enables STP on specified ports.

The following table describes the command parameters.

Parameter	Value	Meaning
`port`	*`<port-list>`*	The ports to enable STP. Specify either a single port or list of ports separated by commas. Example: et.1.3,et.(1-3).(4,6-8)
	`all-ports`	Specifies that all ports are enabled for STP

Restrictions

None

no stp enable port

Mode

Configure

Format

```
no stp enable port <port-list>|all-ports
```

Description

The **no stp enable** command disables STP on specified ports.

The following table describes the command parameters.

Parameter	Value	Meaning
port	*<port-list>*	The ports to disable STP. Specify either a single port or list of ports separated by commas. Example: et.1.3,et.(1-3).(4,6-8)
	all-ports	Specifies that all ports are disabled for STP

Restrictions

None

stp filter-bpdu

Mode

Configure

Format

```
stp filter-bpdu <port-list>
```

Description

The **`stp filter-bpdu`** command is used to filter out BPDUs on a port, when STP is disabled.

The following table describes the command parameters.

Parameter	Value	Meaning
`port`	*`<port-list>`*	The ports on which BPDUs are filtered out when STP is disabled.

Restrictions

None

stp set bridging

Mode

Configure

Format

```
stp set bridging [forward-delay <num>] [hello-time <num>] [max-age <num>] [priority <num>]
[damp-monitor-time <num>] [damp-bpdu-count <num>]
```

Description

The **`stp set bridging`** command is to configure STP operating parameters.

The following table describes the command parameters.

Parameter	Value	Meaning
`forward-delay`	*<num>*	Sets the STP forward delay. The forward delay is measured in seconds. Specify a number from 4– 30. The default is 15.
`hello-time`	*<num>*	Sets the STP hello time. The hello time is measured in seconds. Specify a number from 1– 10. The default is 2.
`max-age`	*<num>*	Sets the STP maximum age. Specify a number from 6–40. The default is 20.
`priority`	*<num>*	Sets the STP bridging priority. Specify a number from 0 – 65535. The default is 32768.
`damp-monitor-time`	*<num>*	Factor of hello time during which a port is monitored to determine if it is stable or unstable. Enter a value between 1 and 20, inclusive. The default is 10.
`damp-bpdu-count`	*<num>*	The number of BPDUs that need to be received within the damp-monitor-time for the link to be considered stable. Enter a value between 1 and 60, inclusive. The default is 10.

Restrictions

None

stp set port

Mode

Configure

Format

```
stp set port <port-list> [[priority <num>[ [port-cost <num>] [dampening enable|disable]]
```

Description

The **`stp set port`** command sets the port priority, port cost and dampening for individual ports.

The following table describes the command parameters.

Parameter	Value	Meaning
`port`	`port <port-list>`	The port(s) to set STP parameters. A single port or a comma-separated list of ports can be specified. Example: et.1.3,et.(1-3),(4,6-8).
`priority`	*<num>*	The priority assiged to the port(s). Specify a number from 0– 255. The default is 128.
`port-cost`	*<num>*	The STP cost assigning to the port(s). Specify a number from 1–65535. The default depends on the port speed: 1 for Gigabit (100-Mbps) ports, 19 for 100-Mbps ports, and 100 for 10-Mbps ports.
`dampening`	`enable`	Enables dampening on the port.
	`disable`	Disables dampening on the port. This is the default.

Restrictions

STP dampening cannot be used in conjunction with RSTP.

stp show bridging-info

Mode

Enable

Format

```
stp show bridging-info
```

Description

The **stp show bridging-info** command displays STP bridging information.

Restrictions

None

Example

This example shows STP bridging information.

```
rs# stp show bridging-info

Status for Spanning Tree Instance 1 :
Bridge ID               : 32768 :001234567800
Root bridge             : 32768 :001234567800
Root Path Cost          : 0
To Root via port        : n/a
Ports in bridge         : 0
Max Age                 : 20 secs
Hello Time              : 2 secs
Forward Delay           : 15 secs
Topology changes        : 0
Last Topology Chg       : 0 days 6 hours 8 min 49 secs ago
```

stp show dampening-info

Mode

Enable

Format

```
stp show dampening-info
```

Description

The **`stp show dampening-info`** command displays the state of ports on which dampening is enabled.

Restrictions

None

Example

This example shows the state of ports on which dampening is enabled.

```
rs# stp show dampening-info
Port Monitor Time (Factor to Hello Time) : 10
Bpdu Count  : 10

Port         Port State
----         -----------
```

stp show protocol-version

Mode

Enable

Format

```
stp show protocol-version
```

Description

The **stp show protocol-version** command displays the spanning tree protocol being used.

Restrictions

None

38 SYSTEM COMMANDS

The **system** commands are used to change and display system parameters.

38.1 COMMAND SUMMARY

The following table lists the **system** commands. The sections following the table describe the command syntax.

system image add [tftp server]<*IPaddr-or-hostname*> <*filename*>
system image list
system image choose [bank0 | bank1]
system kill telnet-session <*session-id*>
system promimage upgrade <hostname-or-IPaddr> <filename>
system set contact <*system-contact*>
system set date year <*year*> month <*month*> day <*day*> hour <*hour*> min <*min*> second <*sec*>
system set idle-timeout telnet <*num*>
system set location <*location*>
system set name <*system-name*>
system set password <*mode*> <*string*> | none
system set terminal baud <*baud-rate*>
system show active-config
system show capacity all|chassis|task|cpu|memory
system show contact
system show date
system show hardware verbose | summary
system show idle-timeout telnet
system set location <*location*>
system show name
system show scratchpad

system show serial-number
system show startup-config
system show terminal
system show uptime
system show users
system show version

system image add

Mode

Enable

Format

```
system image add [tftp server]<IPaddr-or-hostname> <filename>
```

Description

The **`system image add`** command copies a system software image from a TFTP server to the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`add`	`[tftp server]<`	The TFTP server IP address.
	`<IPaddr-or-hostname>`	The IP address.
	`<filename>`	The system software image file name.

Restrictions

None

system image list

Mode

Enable

Format

```
system image list
```

Description

The **`system image list`** command lists the system software image files. The available images (banks) are **`bank0`** and **`bank1`**.

Restrictions

None

system image choose

Mode

Configure

Format

```
system image choose [bank0 | bank1]
```

Description

The **system image choose** command is to specify the system software image file the device uses the next time the system is rebooted. The available images (banks) are **bank0** and **bank1**.

The following table describes the command parameters.

Parameter	Value	Meaning
choose		Specifies which image file is used the next time the system is rebooted.
	Bank0	Specifies that the image file on bank0 is used.
	Bank1	Specifies that the image file on bank1 is used.

Restrictions

None

system kill telnet-session

Mode

Configure

Format

```
system kill telnet-session <session-id>
```

Description

The **system kill telnet-session** command ends the Telnet session specified by the session ID. The **system show users** command is to display the list of current Telnet users and session IDs.

The following table describes the command parameters.

Parameter	Value	Meaning
telnet-session	*<session-id>*	The Telnet session ID number, which can be 0, 1, 2, or 3. The **system show users** command displays the session ID number in the first column. Only one ID session can be specified per **system kill telnet-session** command.

Restrictions

None

system promimage upgrade

Mode

Enable

Format

```
system promimage upgrade <IPaddr-or-hostname> <filename>
```

Description

The **system promimage upgrade** command copies and installs a boot PROM software image from a TFTP server onto the Flash. The boot PROM software image is loaded when the device is powered on.

The following table describes the command parameters.

Parameter	Value	Meaning
upgrade	*<IPaddr-or-hostname>*	The TFTP server or a TFTP URL IP address or host name.
	<filename>	The boot PROM software image file name.

Restrictions

None

system set contact

Mode

Configure

Format

`system set contact <system-contact>`

Description

The **`system set contact`** command specifies the network administrator name and contact information.

The following table describes the command parameters.

Parameter	Value	Meaning
`contact`	*`<system-contact>`*	A string listing the name and contact information for the network administrator responsible for the device. If the string contains blanks or commas, use the quotation marks around the string. (Example: “Jane Doe, janed@corp.com, 408-555-5555 ext. 555”)

Restrictions

None

system set date

Mode

Enable

Format

```
system set date year <year> month <month> day <day> hour <hour> min <min> second <sec>
```

Description

The **system set date** command sets the system time and date. Time is kept with a battery-backed realtime clock. To display the time and date, enter the **system show date** command.

The following table describes the command parameters.

Parameter	Value	Meaning
year	<year>	Four-digit number for the year in the range 1991-2090. (Example: 2001)
month	<month>	Number from 1 – 12 for the month.
day	<day>	Number from 1 – 31 for the day.
hour	<hour>	Number from 0 – 23 for the hour. (The number 0 means midnight.)
min	<min>	Number from 0 – 59 for the hour.
second	<sec>	Number from 0 – 59 for the second.

Restrictions

None

system set idle-timeout

Mode

Configure

Format

`system set idle-timeout telnet <num>`

Description

The **`system set idle-timeout`** command sets the time (in minutes) the console can remain idle before the communication session is terminated by the device.

The following table describes the command parameters.

Parameter	Value	Meaning
`telnet`		This parameter sets the timeout value for a telnet console connection.
	`<num>`	This parameter is to set the idle-timeout value in minutes. Specify any value between 0 and 60. The default is 5 minutes. Specifying 0 disables the timeout.

Restrictions

None

system set location

Mode

Configure

Format

```
system set location <location>
```

Description

The **`system set location`** command creates a string describing the device location. The system name and location can be accessed by SNMP managers.

The following table describes the command parameters.

Parameter	Value	Meaning
`location`	*`<location>`*	A string describing the device location.

Restrictions

None

system set name

Mode

Configure

Format

`system set name <system-name>`

Description

Use the **`system set name`** command to name the device. This name appears in the CLI command prompt.

The following table describes the command parameters.

Parameter	Value	Meaning
`name`	`<system-name>`	The device hostname.

Restrictions

None

system set password

Mode

Configure

Format

```
system set password <mode> <string> | none
```

Description

The **system set password** command sets or changes the passwords for the Login, Enable and Configuration modes.

Note If a password is configured for the Enable mode, a password prompt is displayed the when the **enable** command is entered. Otherwise a message is displayed advising the configuration of an Enable password, then enters the Enable mode. From the Enable mode configuration changes can be made.

The following table describes the command parameters.

Parameter	Value	Meaning
password	*<mode>*	The access mode for which a password is required. Use either **login** or **enable**.
	login	Specifies a password is required to start a CLI session. When the system finishes booting a prompt for a password is displayed.
	enable	The password for entering the Enable mode.
	config	The password for entering the Configuration mode.
	<string>	The password.
	none	If specified, no password is required.

Each mode has a default password. These defaults are as follows:

Mode	Default Password
login	rs
enable	enable
disable	disable
config	config

Restrictions

The passwords are stored in the Startup configuration file. When copying a configuration file from one device to another, the passwords in the file also are copied and are required on the new device.

system set terminal

Mode

Configure

Format

```
system set terminal | baud <baud-rate>
```

Description

The **`system set terminal`** command globally sets parameters for a serial console baud rate.

The following table describes the command parameters.

Parameter	Value	Meaning
baud	*<baud-rate>*	Sets the baud rate.
	9600	9600 baud
	19200	19200 baud
	38400	38400 baud
	115200	115200 baud

Restrictions

None

system show active-config

Mode

Enable

Format

```
system show active-config
```

Description

The **`system show active-config`** command displays the active system CLI configuration.

Restrictions

None

Example

This example shows the active system CLI configuration.

```
rs# system show active-config
Running system configuration:
 1 : interface create ip reshet address-netmask
176.243.37.87/255.255.0.0 port e
t.2.4
 2 : interface create ip rr address-netmask 80.1.1.1 port et.2.23
 3 : interface create ip hamesh address-netmask 90.1.1.1 port et.2.5
 4 : interface create ip rri address-netmask 70.1.1.1 port et.2.6
 5 : interface create ip qa address-netmask 16.1.1.3 port et.2.2
 6 : interface create ip giga address-netmask 100.1.1.1/8 port gi.1.2
 7 : interface create ip re address-netmask 60.1.1.1/8 port et.2.22
 8 : interface create ip wa address-netmask 40.1.1.1 port et.2.10
 9 : interface create ip fs address-netmask 95.1.1.1 port et.2.11
     !
10 : ip add route 176.243.0.0/16 gateway 176.243.1.1
11 : ip add route default gateway 176.243.1.1
     !
12 : port mirroring monitor-port et.2.17 target-port et.2.2
     !
13 : system set location YYY
14 : system set location rs
15 : system set location none
16 : system set location Planet_Earth
17 : system set name rs
```

system show capacity

Mode

Enable

Format

```
system show capacity all |chassis |task |cpu |memory
```

Description

The **`system show capacity`** command displays resource information.

Restrictions

None

Example

This example shows all resource information.

```
rs# system show capacity all
Total     Used        Free      CPU         Power Supply    Switch
Fabric
Slots     Slots       Slots     Redundancy  Redundancy      Redundancy
-----     -----       -----     ----------  -----------     ------------
--
1         1           0         No Support   Support        No Support

Index    Name     Task Status     Memory Used
------   -----    -------------   -----------
  1      IDLE      N/A                 800
  2      IOTG      N/A                 800
  3      IOTM      N/A                1000
  4      SNMP      N/A                5000
  5      BPUP      N/A                1000
  6      HOST      N/A                1000
  7      BRMN      N/A                2000
  8      sdpc      N/A                2000
  9      sarl      N/A                 800
 10      slnk      N/A                 800
 11      tcnt      N/A                2000
 12      dprs      N/A                 800
 13      msyn      N/A                 800
 14      3SHS      N/A                 800
 15      3SFR      N/A                2800
 16      NTPL      N/A                1000
 17      L2HU      N/A                1000
 18      L2PS      N/A                1000
 19      FFTT      N/A                5000
 20      SWDW      N/A                1000
 21      IPAT      N/A                1000
 22      RPTS      N/A                1800
 23      ARPG      N/A                1000
 24       IPG      N/A                1000
 25      ICMP      N/A                1000
 26      TFTP      N/A                1000
 27      IPRD      N/A                1000
 28      PNGA      N/A                1000
 29      UDPR      N/A                1000
```

30	TCPP	N/A	4000
31	ECHO	N/A	1000
32	TNSR	N/A	4000
33	TNSL	N/A	4000
34	POLI	N/A	4000
35	SLIP	N/A	1000
36	XMOD	N/A	1000
37	SCPT	N/A	1000
38	DHCP	N/A	1800
39	DHCp	N/A	1000
40	IPMT	N/A	4000
41	MSCm	N/A	1000
42	STSA	N/A	8000
43	STSB	N/A	8000
44	STSC	N/A	8000
45	STSD	N/A	8000
46	STSE	N/A	8000

system show contact

Mode

Enable

Format

```
system show contact
```

Description

The **system show contact** command displays contact information about the device administrator.

Restrictions

None

Example

This example shows information about the device administrator.

```
rs# system show contact
  Administrative contact: not configured
```

system show date

Mode

Enable

Format

```
system show date
```

Description

The **`system show date`** command displays the system date and time.

Restrictions

None

Example

This example shows the system date and time.

```
rs# system show date
  Current time : 2002-05-12 22:14:36
```

system show hardware

Mode

Enable

Format

```
system show hardware verbose | summary
```

Description

The **`system show hardware`** command displays hardware information. The display includes CPUs, the primary and backup power supplies, and the PC flash card. The information displayed includes cache size, memory size, MAC addresses, and status.

The following table describes the command parameters.

Parameter	Value	Meaning
`hardware`	`verbose`	Displays more detailed information about the system hardware.
	`summary`	Displays summarized information about the system hardware.

Restrictions

None

Example

This example shows hardware information.

```
rs# system show hardware
Hardware Information
System type: ES 500 - Riverstone Networks, Inc. Firmware Version:
1.0.0.1 Prom V
ersion: prom-1.0.0.1 ,Rev.0.4r
CPU Module type:      N.A
Processor:            Type:N.A,Rev. N.A, freq. 266 MHz
  Icache size:        16 Kbytes, 32 bytes/line
  Dcache size         16 Kbytes, 32 bytes/line
CPU Board Frequency:  133 MHz
Backplane Frequency:  N.A
Flash memory:         16 MBytes
System memory size:   64 MBytes
Network memory size:  N.A
MAC Addresses:
  System:             00:12:34:56:78:00
  10/100 CPU Port:    N.A
  Internal use:       N.A
CPU mode:             N.A
Slot information
Port:  et.2.1,  Media Type:  1.0.0.1 ,Rev.0.4r, Physical Port:  1
Port:  et.2.2,  Media Type:  1.0.0.1 ,Rev.0.4r, Physical Port:  2
Port:  et.2.3,  Media Type:  1.0.0.1 ,Rev.0.4r, Physical Port:  3
Port:  et.2.4,  Media Type:  1.0.0.1 ,Rev.0.4r, Physical Port:  4
Port:  et.2.5,  Media Type:  1.0.0.1 ,Rev.0.4r, Physical Port:  5
Port:  et.2.6,  Media Type:  1.0.0.1 ,Rev.0.4r, Physical Port:  6
```

This example shows the system hardware summary information.

```
rs# system show hardware summary
Hardware Information
System type: ES 500 - Riverstone Networks, Inc. Firmware Version:
1.0.0.1 Prom V
ersion: prom-1.0.0.1 ,Rev.0.4r
CPU Module type:      N.A
Processor:            Type:N.A,Rev. N.A, freq. 266 MHz
  Icache size:        16 Kbytes, 32 bytes/line
  Dcache size         16 Kbytes, 32 bytes/line
CPU Board Frequency:  133 MHz
Backplane Frequency:  N.A
Flash memory:         16 MBytes
System memory size:   64 MBytes
Network memory size:  N.A
MAC Addresses:
  System:             00:12:34:56:78:00
  10/100 CPU Port:    N.A
  Internal use:       N.A
CPU mode:             N.A
Slot Information
Slot  1: 2-Gigabit
Slot  2: 24-10/100 Mbit Ethernet
```

system show idle-timeout

Mode

Enable

Format

```
system show idle-timeout telnet
```

Description

The **system show idle-timeout** command displays the timeout value (in minutes). If a session remains idle longer than the **idle-timeout** value, the session is closed by the system. Specify a timeout value for a serial, or a Telnet connection.

Restrictions

None

Example

This example shows the idle timeout value in minutes.

```
rs# system show idle-timeout
serial            - not supported
ssh               - not supported
Telnet console idle timeout = 5 minutes(s)
```

This example shows only the Telnet idle timeout value in minutes.

```
rs# system show idle-timeout telnet
Telnet console idle timeout = 5 minutes(s)
```

system show location

Mode

Enable

Format

```
system show location
```

Description

The **`system show location`** command displays the device location.

Restrictions

None

Example

This example shows the device location.

```
rs# system show location
  System  location: Europe
```

system show name

Mode

Enable

Format

```
system show name
```

Description

The **system show name** command displays the system name.

Restrictions

None

Example

This example shows the device name.

```
rs# system show name
  System  name: rs
```

system show scratchpad

Mode

Enable

Format

```
system show scratchpad
```

Description

The **`system show scratchpad`** command displays the configuration changes in the scratchpad that have not yet been activated.

Restrictions

None

system show serial-number

Mode

Enable

Format

```
system show serial-number
```

Description

The **system show serial-number** command displays the device serial number.

Restrictions

None

Example

This example shows the device serial number.

```
rs# system show serial-number
  System  Serial number id is …….
```

system show startup-config

Mode

Enable

Format

```
system show startup-config
```

Description

The **`system show startup-config`** command displays the startup configuration for the next reboot.

Restrictions

None

Example

This example shows the startup configuration for the next reboot.

```
rs# system show startup-config
!
 ! Startup configuration for the next system reboot
interface create ip reshet address-netmask 176.243.37.87/255.255.0.0
port et.2.4
interface create ip rr address-netmask 80.1.1.1 port et.2.23
interface create ip hamesh address-netmask 90.1.1.1 port et.2.5
interface create ip rri address-netmask 70.1.1.1 port et.2.6
interface create ip qa address-netmask 16.1.1.3 port et.2.2
interface create ip giga address-netmask 100.1.1.1/8 port gi.1.2
interface create ip re address-netmask 60.1.1.1/8 port et.2.22
interface create ip wa address-netmask 40.1.1.1 port et.2.10
interface create ip fs address-netmask 95.1.1.1 port et.2.11
ip add route 176.243.0.0/16 gateway 176.243.1.1
ip add route default gateway 176.243.1.1
port mirroring monitor-port et.2.17 target-port et.2.2
system set location YYY
system set location rs
system set location none
system set location Planet_Earth
system set name rs
snmp set community public privilege read-write
```

system show terminal

Mode

Enable

Format

```
system show terminal
```

Description

The **`system show terminal`** command displays the default terminal baud rate.

Restrictions

None

Example

This example shows default terminal baud rate.

```
rs# system show terminal
Console baud rate is 115200
```

system show uptime

Mode

Enable

Format

```
system show uptime
```

Description

The **`system show uptime`** command displays the time that has elapsed since the last reboot.

Restrictions

None

Example

This example shows time that has elapsed since the last reboot.

```
rs# system show uptime
  System up: 0 day 6 hour 26 min 6 sec
```

system show users

Mode

Enable

Format

```
system show users
```

Description

The **system show users** command displays the current Console and telnet connections.

Restrictions

None

Example

This example shows the current Console and telnet connections.

```
rs# system show users
##                  From              Login Timestamp
----                ----              ---------------
                    console
0T                   176.220.100.12    2002-05-12 21:55:24
```

system show version

Mode

Enable

Format

```
system show version
```

Description

The **`system show version`** command displays the software version running.

Restrictions

None

Example

This example shows the current software version running.

```
Software Information

  Software Version   : 1.0.0.1
  Copyright          : Copyright (c) 2000-2002 Riverstone Networks, Inc.
  Image Information  : Version 1.0.0.1, built on 08-May-2002 23:11:31
  WARNING: This is Controlled Release software.  It is to be
   used in a controlled environment by customers with a
   *pre-arranged agreement* with Riverstone Networks.
   Support for this software expires when the production
   software is officially released.
```

39 VLAN COMMANDS

The **vlan** commands are to perform the following tasks:

- Create VLANs
- List VLANs
- Add ports to VLANs
- Specify ports that cannot be added to a specific VLAN
- Change the port membership of VLANs
- Make a VLAN port either a trunk port, an access port, or a metropolitan area network (MAN) tunnel port

39.1 COMMAND SUMMARY

The following table lists the **vlan** commands. The sections following the table describe the command syntax.

vlan add ports <port-list> to <vlan-name>
vlan create <vlan-name> <type> id <num>
vlan forbid ports <port-list> from <vlan-name>
vlan make access-port <port-list>
vlan make trunk-port <port-list> [exclude-default-vlan]
vlan show

vlan add ports

Mode

Configure

Format

```
vlan add ports <port-list> to <vlan-name>
```

Description

The **`vlan add ports`** command adds ports to an existing VLAN. The VLAN type does not need to be specified when adding ports. The VLAN type is specified when creating the VLAN (using the **`vlan create`** command).

The following table describes the command parameters.

Parameter	Value	Meaning
`ports`	*<port-list>*	The ports to add to the VLAN. A single port or a list of ports separated by commas can be specified. Example: et.1.1, et.1.2, et.1.3 or et.1(1-3)
`to`	*<vlan-name>*	VLAN name to which ports are being adding.

Restrictions

The VLAN to add ports must already exist. To create a VLAN, use the **`vlan create`** command. An access port can be added to only one IP VLAN and one bridged-protocols VLAN.

vlan create

Mode

Configure

Format

```
vlan create <vlan-name> <type> [id <num>]
```

Description

The **vlan create** command creates a VLAN definition. A port-based VLAN or a protocol-based VLAN can be created.

The following table describes the command parameters.

Parameter	Value	Meaning
create	*<vlan-name>*	The VLAN name is a string up to 32 characters long. The VLAN name cannot begin with an underscore (_) or the word "SYS_". The names "control", "default", "blackhole", "reserved", and "learning" cannot be used.
	<type>	The type of VLAN being adding. The VLAN type determines the types of traffic the device forwards on the VLAN. Specify specify **port-base**d.
	port-based	Create this VLAN for all the traffic types listed above (port-based VLAN).
	<num>	VLAN ID. The ID must be unique. Specify a number from 2 – 4094. If more than one device is configured with the same VLAN, the same VLAN ID must be specified on each device.

Note Specify a combination of **ip, appletalk**, **dec**, **sna**, **ipv6**, and **bridged-protocols** or specify **port-based**. The option **port-based** cannot be specified with any of the other options.

Restrictions

The following *cannot* be used for VLAN names:

- control
- default
- blackhole
- reserved
- learning
- names starting with an underscore (_) or "sys_"
- names starting with numeric characters

vlan forbid ports

Mode

Configure

Format

```
vlan forbid ports <port-list> from <vlan-name>
```

Description

The **`vlan forbid ports`** command is to specify those ports which are *not* to be added to a VLAN.

Note This command prevents the specified port from being added to a VLAN, either through the CLI **`vlan add ports`** command or through a facility such as the GARP VLAN Registration Protocol (GVRP), which allows dynamic VLAN creation.

The following table describes the command parameters.

Parameter	Value	Meaning
`ports`	*`<port-list>`*	The ports not be added to the VLAN. A single port or a comma-separated list of ports can be specified. Example: et.1.1, et.1.2, et.1.3 or et.1(1-3)
`to`	*`<vlan-name>`*	VLAN name to which the ports are not added.

Restrictions

None

vlan make access-port

Mode

Configure

Format

```
vlan make access-port <port-list>
```

Description

The **`vlan make access-port`** command turns a port into a VLAN access port. The port forwards traffic only for the VLANs to the configured ports and the traffic will be untagged. This is the default. The port only forwards traffic for VLAN ports with untagged traffic.

The following table describes the command parameters.

Parameter	Value	Meaning
`access-port`	*<port-list>*	The ports being configuring. A single port or a list of ports separated by commas can be specified. Example: et.1.1, et.1.2, et.1.3 or et.1(1-3)

Restrictions

None

vlan make trunk-port

Mode

Configure

Format

```
vlan make trunk-port <port-list>  [exclude-default-vlan]
```

Description

The **`vlan make trunk-port`** command turns a port into a VLAN trunk port. A VLAN trunk port can forward traffic for multiple VLANs. Use trunk ports to connect switches together and send traffic for multiple VLANs on a single network segment connecting the switches. Specify the **`stackable-vlan`** option to designate this trunk port as a tunnel backbone port on which VLAN packets will be tunneled through the metropolitan area network (MAN).

The following table describes the command parameters.

Parameter	Value	Meaning
`trunk-port`	*`<port-list>`*	The ports being configuring. A single port or a list of ports separated by commas can be specified. Example: et.1.1, et.1.2, et.1.3 or et.1(1-3)
`exclude-default-vlan`		Specifies that this trunk port does not belong to the default VLAN.

Restrictions

Packet-over-SONET (PoS) ports must be configured for bridged encapsulation in order to be a VLAN trunk port.

vlan show

Mode

Enable

Format

```
vlan show
```

Description

The **vlan show** command lists all VLANs configured on the device. It provides the following information about each VLAN:

- VLAN ID
- VLAN Name
- VLAN type (determines the traffic types the device forwards on the VLAN)
- Ports included in the VLAN

Restrictions

None

Example

This example shows all VLANs configured on the device.

```
rs# vlan show
VID  VLAN Name                    Used           Ports
---- ---------                   ----           -----
   1 default                     port-based     et.2.(9,11-23),gi.1.(1-2),st.(1-6)
   2 red                         port-based     et.2.(6-8)
```