ZebOS-XP®
Network Platform

Version 1.4
Extended Performance

Network Services Module
Command Reference

December 2015

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Contents

Preface

This document describes the commands for the Network Services Module (NSM) in ZebOS-XP.

Audience

This document is intended for network administrators and other engineering professionals who configure and manage NSM.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, functions, parameters, files, and directories

Contents

This document contains these chapters:

- Chapter 1, *Command Line Interface*
- Chapter 2, *Common Exec Mode Commands*
- Chapter 3, *Common Configure Mode Commands*
- Chapter 4, *Common Router-map Mode Commands*
- Chapter 5, *Interface Commands*
- Chapter 6, *Traffic Engineering Commands*
- Chapter 7, *Control Channel Mode Commands*
- Chapter 8, *Control Adjacency Commands*
- Chapter 9, *Tunneling Commands*
- Chapter 11, *Remote Monitoring Commands*
- Chapter 12, *Unicast Reverse Path Forwarding Check*

Related Documents

The following guides are related to this document:

- *Network Services Module Developer Guide*
- *Installation Guide*

Note: All ZebOS-XP technical manuals are available to licensed customers at http://www.ipinfusion.com/support/document_list.

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

CHAPTER 1 Command Line Interface

This chapter introduces the ZebOS-XP Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain ZebOS-XP devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running ZebOS-XP or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Starting the Command Line Interface

You must start daemons as described in this section before you can use the CLI. The general steps are listed below. For details about the ZebOS-XP daemons, see the *Installation Guide.*

1. Start your terminal emulator and connect to the device or go to the console of the device running ZebOS-XP.
2. Connect to the directory where you installed the ZebOS-XP executables.
3. Start the Network Services Module (NSM).
   ```
   # ./nsm -d
   ```
4. Start the protocol module daemons that your organization uses, such as `mstpd`, `ospf6d`, or `ripd`.
   ```
   # ./mstpd -d
   ```
5. Start the Integrated Management Interface (IMI) daemon.
   ```
   # ./imi -d
   ```
6. Start the IMI shell.
   ```
   # ./imish
   ```
   Note: Your organization may use a ZebOS-XP build that does not include `imish`. If that is the case, you must connect to a port on which a protocol daemon is listening. For details, see the *Installation Guide.*

You can now begin using the CLI.

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

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

```
show ?
  application-priority            Application Priority
```

```
  arp                              Internet Protocol (IP)
  bfd                              Bidirectional Forwarding Detection (BFD)
  bgp                              Border Gateway Protocol (BGP)
  bi-lsp                           Bi-directional lsp status and configuration
  bridge                           Bridge group commands
  ce-vlan                          COS Preservation for Customer Edge VLAN
  class-map                        Class map entry
  cli                              Show CLI tree of current mode
  clns                             Connectionless-Mode Network Service (CLNS)
  control-adjacency                Control Adjacency status and configuration
  control-channel                  Control Channel status and configuration
  cspf                             CSPF Information
  customer                         Display Customer spanning-tree
  cvlan                            Display CVLAN information
  debugging                        Debugging functions (see also 'undebug')
  dot1x                            IEEE 802.1X Port-Based Access Control
  etherchannel                     LACP etherchannel
  ethernet                         Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions (see also 'undebug')
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, ZebOS-XP displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

Command Completion

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

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip         ipv6       isis
> show i
```

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

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

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

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
```



```
>       Output redirection
<cr>
```

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

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh in eth0
```

is an abbreviation for:

```
> show interface eth0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

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

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

If a command is incomplete, the CLI displays the following message:

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

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent
ication-key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table 1-1 describes the conventions used to represent command syntax in this reference.

Table 1-1: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show cli`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show cli`
`UPPERCASE`	See Variable Placeholders	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command. A '?' before a parameter in square brackets limits that parameter to one occurrence in a command string.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table 1-2 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table 1-2: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647>`
`<0-4294967295>`
	Numeric range

Command Description Format

Table 1-3 explains the sections used to describe each command in this reference.

Table 1-3: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Example	An example of the command being executed

Keyboard Operations

Table 1-4 lists the operations you can perform from the keyboard.

Table 1-4: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor

Table 1-4: Keyboard operations (Continued)

Key combination	Operation
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

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

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

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

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either “eth3” or “eth4”:

```
# show run | begin eth[3-4]

...skipping
interface eth3
```

```
 shutdown
!
interface eth4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

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

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

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show int eth0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface eth1 | exclude input
Interface eth1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:


```
# show interface eth0 | exclude (in|out)put
Interface eth0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

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

The output redirection token (>) does the same thing:

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

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table 1-5 lists the command modes common to all protocols.

Table 1-5: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, `list`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as RIP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

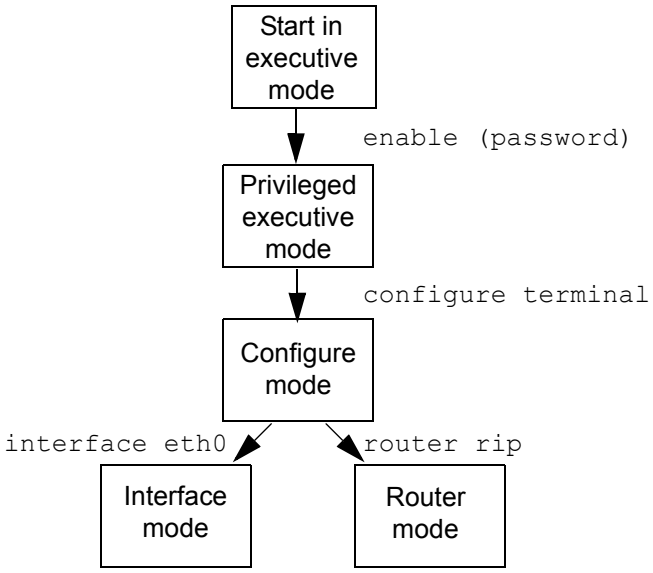

Figure 1-1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows starting `imish` and then moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
# ./imish
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router rip
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

Debug Command

Whether the settings you make for a `debug` command persist between sessions depends on the mode where you make the settings:

- When you make settings for a `debug` command in executive mode, the configuration is valid for the current session only and is not saved in the `ZebOS.conf` file.
- When you make settings for a `debug` command in configuration mode, the configuration is retained and saved in `ZebOS.conf` and used even after the session restarts.

CHAPTER 2 Common Exec Mode Commands

This chapter provides an alphabetized reference for both Exec and Privileged mode commands. All commands are common to multiple NSM protocols. This chapter includes the following commands:

configure terminal

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

Command Syntax

```
configure terminal
```

Parameters

None

Command Mode

Privileged Exec mode

Example

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

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

copy running-config startup-config

Use this command to a write configuration to the file to be used at startup. This is the same as the `write` command (see write on page 62 for more information).

Command Syntax

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

Parameters

None

Command Mode

Privileged Exec mode

Example

```
#copy running-config startup-config
Building configuration...
[OK]
#
```

debug nsm all

Use this command to specify enable all debugging for NSM.

Use the `no` parameter with this command or the undebug command to disable all NSM debugging.

Command Syntax

```
debug nsm (all|)
no debug nsm (all|)
undebug nsm (all|)
```

Parameters

None

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Example

```
#debug nsm all
#
```

debug nsm bfd

Use this command to enabling debugging of BFD (bidirectional forwarding detection) events.

Use the `no` parameter with this command or the undebug command to disable BFD debugging.

Command Syntax

```
debug nsm bfd
no debug nsm bfd
undebug nsm bfd
```

Parameters

None

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Example

```
#debug nsm bfd
#
```

debug nsm events

Use this command to enable debugging of NSM events.

Use the `no` parameter with this command or the undebug command to disable event debugging.

Command Syntax

```
debug nsm events
no debug nsm events
undebug nsm events
```

Parameters

None

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Example

```
#debug nsm events
#
```

debug nsm kernel

Use this command to enable debugging of NSM kernel events.

Use the `no` parameter with this command or the undebug command to disable kernel debugging.

Note: This command is not supported for hardware platform.

Command Syntax

```
debug nsm kernel
no debug nsm kernel
undebug nsm kernel
```

Parameters

None

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Example

```
#debug nsm kernel
#
```

debug nsm packet

Use this command to enable debugging of NSM packet events.

Use the `no` parameter with this command or the undebug command to disable packet debugging.

Command Syntax

```
debug nsm packet (recv|send|) (detail|)
no debug nsm packet (recv|send|) (detail|)
undebug nsm packet (recv|send|) (detail|)
```

Parameters

`recv`	Specify the debug option-set for receive packet.
`send`	Specify the debug option-set for send packet.
`detail`	Sets the debug option to provide detailed information.

Command Mode

Privileged Exec mode, and Configure mode

Example

```
#debug nsm packet
#debug nsm packet recv detail
#
```

disable

Use this command from to exit the Privileged Exec mode and return to the Exec mode. This is the only command that allows a user to go back to the Exec mode. Using the `exit` or `quit` command from the Privileged Exec mode ends the session; they do not go back to the Exec mode.

Command Syntax

```
disable
```

Parameters

None

Command Mode

Privileged Exec mode

Example

```
#disable
>
```

enable

Use this command to enter the Privileged Exec command mode.

Command Syntax

```
enable
```

Parameters

None

Command Mode

Exec mode

Example

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

```
>enable
#
```

end

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

Command Syntax

```
end
```

Parameters

None

Command Mode

All command modes

Example

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

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

exit

Use the exit command to exit the current mode and return to the previous level. When used in Exec mode or Privilege Exec mode, this command terminates the session.

Command Syntax

```
exit
```

Parameters

None

Command Mode

All command modes

Examples

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

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

hardware

Use the `hardware` command to get or set the value to the register.

Note: This command is not supported for ZebIC releases.

Command Syntax

```
hardware register get ADDR
hardware register set ADDR VALUE
```

Parameters

`register`	Specify to get or set the value from the register.
`get`	Specify the register address in 0xhhhh format.
`set`	Specify the register address in 0xhhhh format.

Command Mode

Exec mode and Privilege Exec mode

Example

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

```
#hardware register set 1.1.1.1 new
#hardware register get 1.1.1.1
```

help

Use this command to display help for the ZebOS-XP command line interface (CLI).

Command Syntax

```
help
```

Parameters

None

Command Mode

All command modes

Example

```
#help
ZebOS-XP CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

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

hostname

Use this command to set or change the network server name. ZebOS-XP daemons use this name in system prompts and default configuration filenames. This command provides a hostname for login purposes, only. A hostname could be added for each remote system with which the local router communicates and from which it requires authentication. The other router must have a hostname entry for the local router. This entry must have the same password as the local router.

This command is useful for defining host names for special privileges. For example, a hostname `all` requiring no password could be created allowing the users to connect to general information without a password. Setting a hostname using this command takes precedence over setting a hostname in the kernel. If you set the hostname using the CLI, and then set the hostname in the kernel, the hostname set using the CLI remains.

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

Use the `no` parameter to disable this function.

Command Syntax

```
hostname WORD
no hostname (WORD|)
```

Parameter

`WORD`	This network name for a system.

Command Mode

Pre execution mode

Example

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

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

logout

Use this command to exit from the IMI shell from any of the exec modes.

Command Syntax

```
logout
```

Parameters

None

Command Mode

Exec mode and Privilege Exec mode

Examples

The following examples show the use of `logout` command.

```
>logout
[root@TSUP-123 sbin]#

>enable
#logout
[root@TSUP-123 sbin]#
```

quit

Use the `quit` command to exit the configuration, router or interface modes down to previous mode. When this command is executed in one of the Exec modes, it closes the IMI shell and logs the user out.

Command Syntax

```
quit
```

Parameters

None

Command Mode

All modes

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#quit
(config)#

>enable
#quit
[root@TSUP-123 sbin]#
```

show access-list

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

Command Syntax

```
show access-list
```

Parameters

None

Command Mode

Privileged Exec mode

Example

```
#show access-list

Standard IP access list 13
    permit any
Standard IP access list 67
    deny 1.1.1.0, wildcard bits 0.0.0.255
Extended IP access list 134
    deny ip 1.1.1.0 0.0.0.255 any
ZebOS IP access list 1111
    deny 1.1.1.1/1 exact-match
Standard IP access list 1340
    deny 1.1.1.0, wildcard bits 0.0.0.255
Extended IP access list 2001
    deny ip 1.1.1.0 0.0.0.255 any
ZebOS extended IP access list TK
    deny   tcp 2.2.2.3/24 eq 14 3.3.3.4/24 lt 12 log
ZebOS IP access list mylist
    deny   10.10.0.72/24 exact-match
    permit any
ZebOS extended IP access list new
    deny   icmp any any
ZebOS extended IP access list tk
    deny   tcp 2.2.2.3/24 eq 14 3.3.3.4/24 lt 12 log
#
```

show cli

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

Command Syntax

```
show cli
```

Parameters

None

Command Mode

All command modes

Example

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

```
#show cli
Exec mode:
+-clear
  +-arp-cache [clear arp-cache]
  +-ethernet
    +-cfm
      +-errors
        +-domain
          +-DOMAIN_NAME [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEV
EL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVE
L_ID) (bridge <1-32>|)]
        +-level
          +-LEVEL_ID [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_
ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVE
L_ID) (bridge <1-32>|)]
      +-maintenance-points
        +-remote
          +-domain
            +-DOMAIN_NAME [clear ethernet cfm maintenance-points remote(domain
D
--More--
```

show debugging nsm

Use this command to display debugging information.

Command Syntax

```
show debugging nsm
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Examples

The following is a sample output of the `show debugging nsm` command displaying the NSM debugging status.

```
#show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
#
```

show dot1X

Use this command to display IEEE 802.1x port-based access control information.

Command Syntax

```
show dot1x
show dot1x all
show dot1x diagnostics interface IFNAME
show dot1x interface IFNAME
show dot1x sessionstatistics interface IFNAME
show dot1x statistics interface IFNAME
```

Parameters

`all`	Displays all IEEE 802.1x port-based access control information.
`diagnostics`	Displays diagnostics information.
`interface`	Indicates the interface parameter.
`IFNAME`	Displays the actual interface name.
`sessionstatistics`	Display the statistics for a session.
`statistics`	Display the statistics.

Command Mode

Exec mode and Privileged Exec mode

Example

```
#show dot1x all
802.1X Port-Based Authentication Disabled
  RADIUS client address: not configured
#
```

show history

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

Command Syntax

```
show cli history
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Examples

```
#show cli history
   1 en
   2 show ru
   3 con t
   4 show spanning-tree
   5 exit
```

show ip rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax

```
show ip rpf A.B.C.D
show ip rpf (vrf NAME|) A.B.C.D
```

Parameters

A.B.C.D	IP address of multicast source.
vrf	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Example

```
#show ip rpf 10.10.10.50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

show ipv6 rpf

Use this command to display RPF information for the specified source address.

Command Syntax

```
show ipv6 rpf X:X::X:X
show ipv6 rpf (vrf NAME|) X:X::X:X
```

Parameters

X:X::X:X	IP address of multicast source.
vrf	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Example

```
#show ipv6 rpf 10:10::10:50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

show list

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

Command Syntax

```
show list
```

Parameters

None

Command Mode

All command modes.

Example

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

```
>show list
 clear arp-cache
  clear bgp *
  clear bgp * in
  clear bgp * in prefix-filter
  clear bgp * out
  clear bgp * soft
  clear bgp * soft in
  clear bgp * soft out
  clear bgp <1-4294967295>
  clear bgp <1-4294967295> in
  clear bgp <1-4294967295> in prefix-filter
  clear bgp <1-4294967295> out
  clear bgp <1-4294967295> soft
  clear bgp <1-4294967295> soft in
  clear bgp <1-4294967295> soft out
  clear bgp (A.B.C.D|X:X::X:X)
  clear bgp (A.B.C.D|X:X::X:X) in
  clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
  clear bgp (A.B.C.D|X:X::X:X) out
  clear bgp (A.B.C.D|X:X::X:X) soft
  clear bgp (A.B.C.D|X:X::X:X) soft in
  clear bgp X:X::X:X soft out

--more--
```

show nsm client

Use this command to display NSM client information.

Command Syntax

```
show nsm client
```

Parameters

None

Command Mode

Privileged Exec mode

Example

This command displays the details of currently connected NSM clients, including the services requested by the protocols, statistics and the connection time.

```
#show nsm client
NSM client ID: 1

NSM client ID: 19
 IMI, socket 23
  Service: Interface Service, Router ID Service, VRF Service
  Messsage received 1, sent 58
  Connection time: Thu Jul 22 11:03:12 2010
  Last message read: Service Request
  Last message write: Link Up
NSM client ID: 25
 ONMD, socket 24
  Service: Interface Service, Bridge service, VLAN service
  Messsage received 2, sent 74
  Connection time: Thu Jul 22 11:03:15 2010
  Last message read: OAM  LLDP msg
  Last message write: Link Up
#
```

show privilege

Use the `show privilege` command to display the current privilege level.

Command Syntax

```
show privilege
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of the `show privilege` command displaying the configuration at startup.

```
#show privilege
Current privilege level is 16
#
```

show process

Use the `show process` command to display a process ID, the name of the process, how long the process has been running and any faults detected on the process.

Command Syntax

```
show process
```

Parameters

None

Command Mode

Privileged Exec mode

Example

The following is a sample output of the `show privilege` command displaying the configuration at startup.

```
#show process
 PID NAME             TIME FD
   1 nsm          01:49:24 6

#
```

show running-config router

Use this command to show the running system router configuration.

Command Syntax

```
show running-config router bgp
show running-config router ipv6 ospf
show running-config router ipv6 rip
show running-config router ipv6 vrrp
show running-config router isis
show running-config router ldp
show running-config router ospf
show running-config router rip
show running-config router rsvp
show running-config router vrrp
```

Parameters

`bgp`	Display Border Gateway Protocol (BGP) information.
`ipv6`	Display Internet Protocol version 6 (IPv6) information.
`ospf`	Display Open Shortest Path First (OSPF) information for an IPv6 interface.
`rip`	Display Routing Information Protocol (RIP) information for an IPv6 interface.
`vrrp`	Display Virtual Router Redundancy Protocol (VRRP) information for an IPv6 interface.
`isis`	Display Intermediate System to Intermediate System (IS-IS) information.
`ldp`	Display Label Distribution Protocol (LDP) information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`rsvp`	Display Resource Reservation Protocol (RSVP) information.
`vrrp`	Display Virtual Router Redundancy Protocol (VRRP) information.

Command Mode

Privileged Exec mode, Configure mode, Router-map mode

Example

```
>enable
#show running-config router vrrp
!
router-id 3.3.3.3
!
```

show running-config switch

Use this command to show the running system status and configuration details for a given switch.

Command Syntax

```
show running-config switch bridge
show running-config switch dot1x
show running-config switch gmrp
show running-config switch gvrp
show running-config switch lacp
show running-config switch lmi
show running-config switch mstp
show running-config switch radius-server
show running-config switch rpsvt+
show running-config switch rstp
show running-config switch ptp
show running-config switch stp
show running-config switch synce
show running-config switch vlan
```

Parameters

`bridge`	Display Bridge group information.
`dot1x`	Display 802.1x port-based authentication information.
`gmrp`	Display GARP Multicast Registration Protocol (GMRP) information.
`gvrp`	Display GARP VLAN Registration Protocol (GVRP) information.
`lacp`	Display Link Aggregation Control Protocol (LACP) information.
`lmi`	Display Ethernet Local Management Interface Protocol (LMI) information.
`mstp`	Display Multiple Spanning Tree Protocol (MSTP) information.
`radius-server`	Display RADIUS server information.
`rpvst+`	Display Rapid Per-VLAN Spanning Tree (rpvst+) information.
`rstp`	Display Rapid Spanning Tree Protocol (RSTP) information.
`ptp`	Display Precision time Protocol (PTP)
`stp`	Display Spanning Tree Protocol (STP) information.
`synce`	Display synce information.
`vlan`	Display values associated with a single VLAN.

Command Mode

Privileged Exec mode, Configure mode, Router-map mode

Example

```
(config)#show running-config switch stp
!
bridge 6 ageing-time 45
bridge 6 priority 4096
bridge 6 max-age 7
```

show startup-config

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

Command Syntax

```
show startup-config
```

Parameters

None

Command Mode

Privileged Exec mode

Example

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

```
#show startup-config
! ZebOS configuration saved from vty
!   2001/04/21 11:38:52
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 redistribute connected
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line vty
 exec-timeout 0 0
```

show static-channel-group

Use this command to display the types of load-balancing port selection criteria (PSC) used on configured static aggregators.

Command Syntax

```
show static-channel-group
```

Parameters

None

Command Mode

Privileged Exec mode

Examples

The following is an example of the output of this command:

```
# show static-channel-group
% Static Aggregator: sa200
Source and Destination Mac address
% Static Aggregator: sa201
Destination IP address
```

show users

Use this command to display information about terminal lines.

Command Syntax

```
show users
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

This is a sample output of the `show users` command:

```
#show users

Line       User       Host(s)              Idle       Location
130 vty 0             idle                 00:45:44   2
#
```

show user-priority

Use this command to display the default user priority associated with the layer2 interface

Command Syntax

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

Parameters

`interface`	Indicates the interface parameter.
`IFNAME`	Indicates the actual interface name.

Command Mode

Exec mode and Privileged Exec mode

Example

```
#show user-priority interface eth1
#
```

show user-priority-regen-table

Use this command to display the user priority that is used to regenerate user-priority mapping, which is associated with a layer 2 interface.

Command Syntax

```
show user-priority-regen-table interface IFNAME
```

Parameters

`interface`	Indicates the interface parameter.
`IFNAME`	Indicates the actual interface name.

Command Mode

Exec mode and Privileged Exec mode

Example

This is a sample output of the `show users` command:

```
#show user-priority-regen-table interface eth1
```

show version

Use the `show version` command to display the version information for ZebOS-XP.

Command Syntax

```
show version
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

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

```
#show version
ZebOS SRS 6.1 (i686-pc-linux-gnu) 12172003
Copyright 2001-2003 IP Infusion Inc.

NET-SNMP SNMP agent software
(c) 1989, 1991, 1992 by Carnegie Mellon University;
(c) 1996, 1998-6.10 The Regents of the University of California.
All Rights Reserved;
(c) 6.11, Networks Associates Technology, Inc. All rights reserved;
(c) 6.11, Cambridge Broadband Ltd. All rights reserved.
 RSA Data Security, Inc. MD5 Message-Digest Algorithm
(c) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
Libedit Library
(c) 1992, 1993 The Regents of the University of California. All rights
reserved.
OpenSSL Library
Copyright (C) 1998-6.12 The OpenSSL Project. All rights reserved.
Original SSLeay License
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
```

terminal length

Use the `terminal length` command to set number of lines displayed on a terminal.

Command Syntax

```
terminal length <0-511>
```

Parameters

`<0-511>`	The number of lines on a terminal. The default length is 25 lines.

Command Mode

Exec mode and Privileged Exec mode

Examples

The following example sets the terminal length to 30 lines.

```
#terminal length 30
```

terminal monitor

Use this command to enable viewing debug messages on the terminal. When the command is used without either of the optional parameters, it may be used by a PVR user or non-PVR user and enables debug output on the terminal for the current VR context. When used with either parameter, it may be used only by a PVR user.

Command Syntax

```
terminal monitor (all|WORD|)
```

Parameters

`WORD`	Used in the PVR context, and contains the VR name to be included in the debugging session.
`all`	Used the PVR context to include all VR in a PVR debugging session.

Command Mode

Privileged Exec mode

Example

```
#terminal monitor
```

who

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

Note: This command is unavailable if you are running using `imish`. In addition, this command is only available on Linux.

Command Syntax

```
who
```

Parameters

None

Command Mode

Privileged Exec mode

Example

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

```
#who
 root     tty1         2015-09-14 14:20
root     pts/0        2015-09-14 14:44 (10.12.7.76)
```

write

Use this command to write configuration data to a file.

Command Syntax

```
write file
write memory
```

Parameters

`file`	Specify to write the configuration to a file.
`memory`	Specify to write the configuration write to non-volatile (NV) memory.

Command Mode

Privileged Exec mode

Example

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

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

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

```
#write memory
Building configuration...
[OK]
```

write terminal

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

Command Syntax

```
write terminal
```

Parameters

None

Command Mode

Privileged Exec mode

Example

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

```
#write terminal

Current configuration:
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
 redistribute connected
!
line vty
 exec-timeout 0 0
```

CHAPTER 3 Common Configure Mode Commands

This chapter provides an alphabetized reference for the Configure mode commands. Commands are common to multiple NSM protocols. This chapter includes the following commands:

access-list WORD

Use this command to configure an access-list (ACL) to filter packets. This command controls the transmission of packets on an interface and restrict contents of routing updates. The switch stops checking the access list after a match occurs. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Note: When using this command from a Telnet session, be sure to telnet to the specific protocol daemon (for example, isisd). Unpredictable results may occur if this command is used in a telnet session with the NSM daemon.

Command Syntax

```
access-list WORD (deny|permit) A.B.C.D/M
access-list WORD (deny|permit) A.B.C.D/M exact-match
access-list WORD (deny|permit) any
no access-list WORD (deny|permit) A.B.C.D/M
no access-list WORD (deny|permit) A.B.C.D/M exact-match
no access-list WORD (deny|permit) any
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to reject.
`permit`	Specify route to permit.
`A.B.C.D/M`	An IP address and mask specifying which part of the IP address will be ignored.
`any`	Allows any IP address or prefix to match.
`exact-match`	Specify an exact matching of prefixes.
`remark`	Access list entry comment.
`LINE`	Multi-line, access-list entry comment up to 100 characters.

Command Mode

Configure mode

Examples

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

access-list (Extended Range)

Use this command to configure an access-list (ACL) to filter packets in an extended range. This command controls the transmission of packets on an interface and restrict contents of routing updates. The switch stops checking the access list after a match occurs. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Note: When using this command from a Telnet session, be sure to telnet to the specific protocol daemon (for example, isisd). Unpredictable results may occur if this command is used in a telnet session with the NSM daemon.

Command Syntax

```
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D A.B.C.D
  A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D any
access-list (<100-199>|<2000-2699>) (deny|permit) ip any A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip any any
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip any host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D any
no access-list (100-199>|<2000-2699>|WORD) remark LINE
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D A.B.C.D
  A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D any
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any any
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D host
  A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D A.B.C.D
  A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D host A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any host A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D any
no access-list (100-199>|<2000-2699>|WORD) remark LINE
```

Parameters

`<100-199>`	IP extended access list.
`<2000-2699>`	IP extended access list (expanded range).
`deny`	Specify route to reject.
`permit`	Specify route to permit.
`ip`	Specify any Internet Protocol.
`A.B.C.D`	An IP address and mask specifying which part of the IP address will be ignored.
`any`	Allows any IP address or prefix to match.
`host`	Specify a single source host.
`remark`	Access list entry comment.
`LINE`	Multi-line, access-list entry comment up to 100 characters.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#access-list 134 deny ip 1.1.1.0 0.0.0.255 any

(config)#access-list 1340 deny 1.1.1.0 0.0.0.255
```

access-list (Standard Range)

Use this command to configure an access-list (ACL) to filter packets in an standard range. This command controls the transmission of packets on an interface and restrict contents of routing updates. The switch stops checking the access list after a match occurs. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Note: When using this command from a Telnet session, be sure to telnet to the specific protocol daemon (for example, isisd). Unpredictable results may occur if this command is used in a telnet session with the NSM daemon.

Command Syntax

```
access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) any
access-list (<1-99>|<1300-1999>|WORD) remark LINE
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) any
```

Parameters

`<1-99>`	IP standard access list
`<1300-1999>`	IP standard access list (expanded range).
`deny`	Specify route to reject.
`permit`	Specify route to permit.
`A.B.C.D`	An IP address and mask specifying which part of the IP address will be ignored.
`any`	Allows any IP address or prefix to match.
`remark`	Access list entry comment.
`LINE`	Multi-line, access-list entry comment up to 100 characters.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#access-list 67 deny 1.1.1.0 0.0.0.255
(config)#access-list 13 permit any
```

access-list zebos

Use this command to configure an access-list (ACL) to filter packets. This command controls the transmission of packets on an interface and restrict contents of routing updates. The switch stops checking the access list after a match occurs. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Note: When using this command from a Telnet session, be sure to telnet to the specific protocol daemon (for example, isisd). Unpredictable results may occur if this command is used in a telnet session with the NSM daemon.

Command Syntax

```
access-list zebos WORD (deny|permit) (ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-
  255>) (A.B.C.D/M|A.B.C.D A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any) ({label <1-
  65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`<0-255>`	Specify a number to identify a protocol, instead of a named protocol (as listed below).
`any`	Specify any protocol packet.
`gre`	Specify Generic Routing Encapsulation packet.
`igmp`	Specify Internet Group Management Protocol packet.
`ip`	Specify IP packet.
`ipcomp`	Specify IP payload compression packet.
`ospf`	Specify Open Shortest Path First packet.
`pim`	Specify Protocol Independent Multicast packet.
`rsvp`	Specify Resource Reservation Protocol packet.
`vrrp`	Specify Virtual Router Redundancy Protocol packet.
`A.B.C.D`	Source IP address.
`A.B.C.D/M`	Source IP address and mask.
`any`	Source any local address.
`A.B.C.D`	Destination IP address.
`A.B.C.D/M`	Destination IP address and mask.
`any`	Destination any local address.

`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.
`interface`	Indicate the `interface` keyword, which is the name of the input or output interface.
`in`	Specify the actual input interface.
`out`	Specify the actual output interface.
`IFNAME`	Specify the actual interface name.
`label`	Indicate the `label` keyword, which is used to identify an application.
`<1-65535>`	Specify the actual label value.
`log`	Log the results.
`pkt-size`	Indicate the `packet` keyword, which is used to identify packet size.
`gt`	Packet size less than or greater than specified value.
`lt`	Packet size less than or greater than specified value.
`range`	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
`<0-65535>`	Specify the actual range of values for packet size from <0-65535>.
`precedence`	Indicate the `precedence` keyword, which is used to identify a packet filter precedence level.
`<0-7>`	Specify the precedence value.
`tos`	Type of service (ToS) value; also used to filter packets.
`<0-255>`	Specify the actual value for ToS.
`range`	Indicate the `range` keyword.
`<0-255>`	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#access-list zebos tk permit any any any fragments interface in eth1
```

access-list zebos icmp

Use this command to configure an access-list (ACL) to filter packets specific to the ICMP protocol. This command controls the transmission of packets on an interface and restrict contents of routing updates. The switch stops checking the access list after a match occurs. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Note: When using this command from telnet, be sure to telnet to the specific protocol daemon (for example, isisd). Unpredictable results may occur if this command is used in a telnet session with the NSM daemon.

Command Syntax

```
access-list zebos WORD (deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
  (A.B.C.D/M|A.B.C.D A.B.C.D|any) ({icmp-type ICMP-TYPE|label <1-65535>|precedence
  <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt) <0-65535>|range <0-
  65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
no access-list zebos WORD (deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
  (A.B.C.D/M|A.B.C.D A.B.C.D|any) ({icmp-type ICMP-TYPE|label <1-65535>|precedence
  <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt) <0-65535>|range <0-
  65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`icmp`	Specify Internet Control Message Protocol packet.
`A.B.C.D`	Source IP address.
`A.B.C.D/M`	Source IP address and mask.
`any`	Source any local address.
`A.B.C.D`	Destination IP address.
`A.B.C.D/M`	Destination IP address and mask.
`any`	Destination any local address.
`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.
`icmp-type`	Indicate the `icmp-type` keyword, which is used to specify the ICMP type.
`ICMP-TYPE`	Specify the actual ICMP value.
`interface`	Indicate the `interface` keyword, which is the name of the input or output interface.
`in`	Specify the actual input interface.
`out`	Specify the actual output interface.

IFNAME	Specify the actual interface name.
label	Indicate the label keyword, which is used to identify an application.
<1-65535>	Specify the actual label value.
log	Log the results.
pkt-size	Indicate the packet keyword, which is used to identify packet size.
gt	Packet size less than or greater than specified value.
lt	Packet size less than or greater than specified value.
range	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
<0-65535>	Specify the actual range of values for packet size from <0-65535>.
precedence	Indicate the precedence keyword, which is used to identify a packet filter precedence level.
<0-7>	Specify the precedence value.
tos	Type of service (ToS) value; also used to filter packets.
<0-255>	Specify the actual value for ToS.
range	Indicate the range keyword.
<0-255>	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#access-list zebos tk deny icmp any any icmp-type new-ICMP fragments
log
```

access-list zebos tcp

Use this command to configure an access-list (ACL) to filter packets specific to the TCP protocol. This command controls the transmission of packets on an interface and restrict contents of routing updates. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Note: When using this command from telnet, be sure to telnet to the specific protocol daemon (for example, isisd). Unpredictable results may occur if this command is used in a telnet session with the NSM daemon.

Command Syntax

```
access-list zebos WORD (deny|permit) (tcp) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
  ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D
  |any) ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) ({established |label
  <1-65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
no access-list zebos WORD (deny|permit) (tcp) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
  ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D
  |any) ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) ({established|label
  <1-65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`tcp`	Specify Transmission Control Protocol packet.
`A.B.C.D`	Source IP address.
`A.B.C.D/M`	Source IP address and mask.
`any`	Source any local address.
`A.B.C.D`	Destination IP address.
`A.B.C.D/M`	Destination IP address and mask.
`any`	Destination any local address.
`eq`	Indicate the `eq` keyword, which specifies a destination port as equal to a given value.
`<0-65535>`	Specify the actual equal than value.
`established`	Indicate the `established` keyword, which is used to specify that an address is an established connection.
`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.
`gt`	Indicate the `gt` keyword, which specifies a destination port as greater than a given value.

<0-65535>	Specify the actual greater than value.
interface	Indicate the interface keyword, which is the name of the input or output interface.
in	Specify the actual input interface.
out	Specify the actual output interface.
IFNAME	Specify the actual interface name.
label	Indicate the label keyword, which is used to identify an application.
<1-65535>	Specify the actual label value.
lt	Indicate the lt keyword, which specifies a destination port as less than a given value.
<0-65535>	Specify the actual less than value.
log	Log the results.
ne	Indicate the ne keyword, which specifies a destination port as not equal to a given value.
<0-65535>	Specify the actual not equal than value.
pkt-size	Indicate the packet keyword, which is used to identify packet size.
gt	Packet size less than or greater than specified value.
lt	Packet size less than or greater than specified value.
range	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
<0-65535>	Specify the actual range of values for packet size from <0-65535>.
precedence	Indicate the precedence keyword, which is used to identify a packet filter precedence level.
<0-7>	Specify the precedence value.
tos	Type of service (ToS) value; also used to filter packets.
<0-255>	Specify the actual value for ToS.
range	Indicate the range keyword.
<0-255>	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#access-list zebos tk deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24 lt 12 log
```

access-list zebos udp

Use thiscommand to configure an access-list (ACL) to filter packets specific to the UDP protocol. This command controls the transmission of packets on an interface and restrict contents of routing updates. The switch stops checking the access list after a match occurs. The priority of an ACL is based on the order in which the access-list command was configured. For example:

- If the user configures the ACL as “deny,” the label does not advertise to any peer.
- If the user configures the ACL as “no-match,” then it applies the next advert-list and is interpreted as continue.
- If the user configures the ACL as “permit” and there is a peer ACL, then the label advertises to all peers permitted by the peer ACL.
- If the user configures the ACL as “permit,” but the peer prefix is “none,” then the label advertises to all peers.

Use the `no` parameter to remove a specified access-list.

Command Syntax

```
access-list zebos WORD (deny|permit) (udp) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
  ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D
  A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) ({label <1-
  65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
no access-list zebos WORD (deny|permit) (udp) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
  ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D
  A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> |range <0-65535> <0-65535>|) ({label <1-
  65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`udp`	Specify User Datagram Protocol packet.
`A.B.C.D`	Source IP address.
`A.B.C.D/M`	Source IP address and mask.
`any`	Source any local address.
`A.B.C.D`	Destination IP address.
`A.B.C.D/M`	Destination IP address and mask.
`any`	Destination any local address.
`eq`	Indicate the `eq` keyword, which specifies a source port as equal to a given value.
`<0-65535>`	Specify the actual equal to value.
`gt`	Indicate the `gt` keyword, which specifies a source port as greater than a given value.
`<0-65535>`	Specify the actual greater than value.
`lt`	Indicate the `lt` keyword, which specifies a source port as less than a given value.
`<0-65535>`	Specify the actual less than value.
`ne`	Indicate the `gt` keyword, which specifies a source port as not equal to a given value.

<0-65535>	Specify the actual not equal to value.
range	Indicate the range keyword, which is used to specify the range of a source port.
<0-255>	Specify the actual range of the source port from <0 to 255>.
eq	Indicate the eq keyword, which specifies a destination port as equal to a given value.
<0-65535>	Specify the actual equal to value.
fragments	Indicate the fragments keyword. An ACL applies to the non-initial fragment of packet.
gt	Indicate the gt keyword, which specifies a destination port as greater than a given value.
<0-65535>	Specify the actual greater than value.
interface	Indicate the interface keyword, which is the name of the input or output interface.
in	Specify the actual input interface.
out	Specify the actual output interface.
IFNAME	Specify the actual interface name.
label	Indicate the label keyword, which is used to identify an application.
<1-65535>	Specify the actual label value.
log	Log the results.
lt	Indicate the lt keyword, which specifies a destination port as less than a given value.
<0-65535>	Specify the actual less than value.
ne	Indicate the ne keyword, which specifies a destination port as less than a given value.
<0-65535>	Specify the actual not equal than value.
pkt-size	Indicate the packet keyword, which is used to identify packet size.
gt	Packet size less than or greater than specified value.
lt	Packet size less than or greater than specified value.
range	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
<0-65535>	Specify the actual range of values for packet size from <0-65535>.
precedence	Indicate the precedence keyword, which identifies a packet filter precedence level.
<0-7>	Specify the precedence value.
range	Indicate the range keyword, which is used to specify the range of a destination port.
<0-255>	Specify the actual range of the destination port from <0 to 255>.
tos	Type of service (ToS) value; also used to filter packets.
<0-255>	Specify the actual value for ToS.
range	Indicate the range keyword.
<0-255>	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
(config)#access-list zebos tk deny udp 2.2.2.3/24 eq 14 3.3.3.4/24 lt 12
```

arp

Use this command to create a static group ARP entry.

Use the `no` parameter to remove the static group ARP entry.

Command Syntax

```
ip arp A.B.C.D MAC (alias|)
no ip arp A.B.C.D
```

Parameters

`A.B.C.D`	Specify the IP address of the ARP entry.
`MAC`	Specify the MAC (hardware) address of the ARP entry in HHHH.HHHH.HHHH format.
`alias`	Specify the response to ARP requests for the IP address.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ip arp 10.10.10.10 0010.2355.4566 alias

(config)#no ip arp 10.10.10.10
```

enable password

Use the `enable password` command to modify or create a password to be used when entering the `Enable` mode. There are three methods to enable a password:

Plain Password

The plain password is a clear text string that appears in the configuration file as configured.

Encrypted Password

An encrypted password encrypts a password. First, use the enable password command to create a password. Then, use the `service encrypted-password` command to encrypt the specified string. An encrypted password does not display in the configuration file; instead, it displays the encrypted string.

Note: See service password-encryption on page 96 for more information on hidden passwords

Hidden Password

A hidden password also encrypts a password; however, you do not need the `service password-encryption` command for this method. Use this method if you know the encrypted string of the plain text string that you want to use as a password. The output in the configuration file displays only the encrypted string and not the text string

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

Use the `no` parameter to disable the password.

Command Syntax

```
enable password (8|) LINE
no enable password
no enable password LINE
```

Parameters

`8`	Specify that a hidden password will follow.
`line`	Specify the hidden enable password string.

Note: Password can be an alpha-numeric string up to 80-characters, including spaces. The string cannot begin with a number.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#enable password mypasswd

#configure terminal
(config)#enable password 8 fU7zHzuutY2SA
```

ip mroute

Use this command to create a multicast static route. Use the `no` form of this command to clear the route. Multicast static routes are unicast routes which allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform reverse-path forwarding (RPF) checks.

Use the `no` form of this command to clear the route.

Command Syntax

```
ip mroute A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE)
ip mroute A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE) <1-255>
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE)
ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE) <1-
  255>
no ip mroute A.B.C.D/M (static|rip|ospf|bgp|isis|)
no ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|)
```

Parameters

`A.B.C.D/M`	Specify multicast source IP address and mask
`A.B.C.D`	RPF address for the multicast route. Host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up to one level.
`INTERFACE`	Incoming interface name. Can only be specified for non-broadcast interfaces.
`bgp`	Specify the border gateway protocol (BGP).
`isis`	Specify the Intermediate system to intermediate system (IS-IS) protocol.
`ospf`	Specify the open shortest patch first (OSPF) protocol.
`rip`	Specify the routing information protocol (RIP) protocol.
`static`	Specify a static route.
`A.B.C.D`	Specify reverse path forwarding (RPF) neighbor address or route.
`INTERFACE`	Specify reverse path forwarding (RPF) interface or pseudo interface.
`<1-255>`	Specify whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. Default is 0.
`vrf`	Specify the VRF name for the static route.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ip mroute 10.10.10.50/1 255.255.255.0 1

#configure terminal
(config)#ip mroute vrf VRF_A 10.10.10.50/1 255.255.255.0 1
```

ipv6 access-list

Use this command to configure an access list for filtering frames.

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

Use the `no` parameter to remove a specified access-list.

Note: This command is unavailable if you are running `imish`. To control access from the network/ hosts, you must change system files, such as `/etc/host.allow` and `/etc/hosts.deny`.

Command Syntax

```
ipv6 access-list WORD (deny|permit) X:X::X:X/M
ipv6 access-list WORD (deny|permit) X:X::X:X/M exact-match
ipv6 access-list WORD (deny|permit) any
ipv6 access-list WORD remark LINE
no ipv6 access-list WORD (deny|permit) X:X::X:X/M
no ipv6 access-list WORD (deny|permit) X:X::X:X/M exact-match
no ipv6 access-list WORD (deny|permit) any
no ipv6 access-list WORD
no ipv6 access-list WORD remark
```

Parameters

`WORD`	Access-list name
`DENY`	Specify route to reject.
`PERMIT`	Specify route to permit.
`X:X::X:X/M`	An IP address and mask specifying which part of the IP address will be ignored.
`any`	Allows any IP address or prefix to match.
`exact-match`	Specify an exact matching of prefixes.
`REMARK`	Access list entry comment.
`LINE`	Multi-line, access-list entry comment up to 100 characters.

Command Mode

Configure mode and Line mode

Examples

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

#configure terminal
(config)#line vty 12 77
(config-line)#ipv6 access-class mylist1
```

ipv6 access-list zebos

Use this command to configure an access list for filtering frames that permit or deny multiple IANA protocols. An access list controls the transmission of packets on an interface, and restrict the content of routing updates. The switch stops checking the access list when a match is encountered.

Some protocols are identified by name, such as IP, GRE, or TCP packets. Other are identified by a number in the range of <0-255>. Use mask to specify a subset of addresses. Use `any` to allow all packets.

Use the `no` option with any of the `access-list zebos` command variants to remove a specified access-list.

Command Syntax

```
ipv6 access-list zebos WORD (deny|permit)
  (ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) (X:X::X:X/M|X:X::X:X X:X::X:X|any) ({label <1-65535>|precedence <0-
  7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt) <0-65535>|range <0-
  65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
no ipv6 access-list zebos WORD ((deny|permit)
  (ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) (X:X::X:X/M|X:X::X:X X:X::X:X|any) ({label <1-65535>|precedence <0-
  7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt) <0-65535>|range <0-
  65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`<0-255>`	Specify a number to identify a protocol, instead of a named protocol (as listed below).
`any`	Specify any protocol packet.
`gre`	Specify Generic Routing Encapsulation packet.
`igmp`	Specify Internet Group Management Protocol packet.
`ip`	Specify IP packet.
`ipcomp`	Specify IP payload compression packet.
`ospf`	Specify Open Shortest Path First packet.
`pim`	Specify Protocol Independent Multicast packet.
`rsvp`	Specify Resource Reservation Protocol packet.
`vrrp`	Specify Virtual Router Redundancy Protocol packet.
`X:X::X:X`	Source IPv6 address.
`X:X::X:X/M`	Source IPv6 address and mask.
`any`	Source any local address.
`X:X::X:X`	Destination IPv6 address.
`X:X::X:X/M`	Destination IPv6 address and mask.
`any`	Destination any local address.
`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.

`interface`	Indicate the `interface` keyword, which is the name of the input or output interface.
`in`	Specify the actual input interface.
`out`	Specify the actual output interface.
`IFNAME`	Specify the actual interface name.
`label`	Indicate the `label` keyword, which is used to identify an application.
`<1-65535>`	Specify the actual label value.
`log`	Log the results.
`pkt-size`	Indicate the `packet` keyword, which is used to identify packet size.
`gt`	Packet size less than or greater than specified value.
`lt`	Packet size less than or greater than specified value.
`range`	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
`<0-65535>`	Specify the actual range of values for packet size from <0-65535>.
`precedence`	Indicate the `precedence` keyword, which is used to identify a packet filter precedence level.
`<0-7>`	Specify the precedence value.
`tos`	Type of service (ToS) value; also used to filter packets.
`<0-255>`	Specify the actual value for ToS.
`range`	Indicate the `range` keyword.
`<0-255>`	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#ipv6 access-list zebos TK deny any any any fragments interface out
eth1 log
```

ipv6 access-list zebos icmp

Use this command to configure an access list for filtering frames that permit or deny multiple IANA protocols. An access list controls the transmission of packets on an interface, and restrict the content of routing updates. The switch stops checking the access list when a match is encountered.

Some protocols are identified by name, such as IP, GRE, or TCP packets. Other are identified by a number in the range of <0-255>. Use mask to specify a subset of addresses. Use `any` to allow all packets.

Use the `no` option with any of the `access-list zebos` command variants to remove a specified access-list.

Command Syntax

```
ipv6 access-list zebos WORD (deny|permit) (icmp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) ({icmp-type ICMP-TYPE|label <1-
  65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
no ipv6 access-list zebos WORD (deny|permit) (icmp) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) (X:X::X:X/M|X:X::X:X X:X::X:X|any) ({icmp-type ICMP-TYPE|label <1-
  65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`icmp`	Specify Internet Control Message Protocol packet.
`X:X::X:X`	Source IP address.
`X:X::X:X/M`	Source IP address and mask.
`any`	Source any local address.
`X:X::X:X`	Destination IP address.
`X:X::X:X/M`	Destination IP address and mask.
`any`	Destination any local address.
`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.
`icmp-type`	Indicate the `icmp-type` keyword, which is used to specify the ICMP type.
`ICMP-TYPE`	Specify the actual ICMP value.
`interface`	Indicate the `interface` keyword, which is the name of the input or output interface.
`in`	Specify the actual input interface.
`out`	Specify the actual output interface.
`IFNAME`	Specify the actual interface name.
`label`	Indicate the `label` keyword, which is used to identify an application.
`<1-65535>`	Specify the actual label value.
`log`	Log the results.
`pkt-size`	Indicate the `packet` keyword, which is used to identify packet size.
`gt`	Packet size less than or greater than specified value.

`lt`	Packet size less than or greater than specified value.
`range`	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
`<0-65535>`	Specify the actual range of values for packet size from <0-65535>.
`precedence`	Indicate the `precedence` keyword, which is used to identify a packet filter precedence level.
`<0-7>`	Specify the precedence value.
`tos`	Type of service (ToS) value; also used to filter packets.
`<0-255>`	Specify the actual value for ToS.
`range`	Indicate the `range` keyword.
`<0-255>`	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#ipv6 access-list zebos TK deny icmp 2::2/64 any icmp-type new_icmp
log
```

ipv6 access-list zebos tcp

Use this command to configure an access list for filtering frames that permit or deny multiple IANA protocols. An access list controls the transmission of packets on an interface, and restrict the content of routing updates. The switch stops checking the access list when a match is encountered.

Some protocols are identified by name, such as IP, GRE, or TCP packets. Other are identified by a number in the range of <0-255>. Use mask to specify a subset of addresses. Use `any` to allow all packets.

Use the `no` option with any of the `access-list zebos` command variants to remove a specified access-list.

Command Syntax

```
ipv6 access-list zebos WORD (deny|permit) (tcp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|)
  ({established|label <1-65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-
  255>)|pkt-size ((lt|gt) <0-65535>|range <0-65535> <0-
  65535>)|fragments|log|interface (in|out) IFNAME}|)
no ipv6 access-list zebos WORD (deny|permit) (tcp) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|)
  ({established|label <1-65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-
  255>)|pkt-size ((lt|gt) <0-65535>|range <0-65535> <0-
  65535>)|fragments|log|interface (in|out) IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`tcp`	Specify Transmission Control Protocol packet.
`X:X::X:X`	Source IP address.
`X:X::X:X/M`	Source IP address and mask.
`any`	Source any local address.
`X:X::X:X`	Destination IP address.
`X:X::X:X/M`	Destination IP address and mask.
`any`	Destination any local address.
`eq`	Indicate the `eq` keyword, which specifies a destination port as equal to a given value.
`<0-65535>`	Specify the actual equal than value.
`established`	Indicate the `established` keyword, which is used to specify that an address is an established connection.
`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.
`gt`	Indicate the `gt` keyword, which specifies a destination port as greater than a given value.
`<0-65535>`	Specify the actual greater than value.
`interface`	Indicate the `interface` keyword, which is the name of the input or output interface.
`in`	Specify the actual input interface.

out	Specify the actual output interface.
IFNAME	Specify the actual interface name.
label	Indicate the label keyword, which is used to identify an application.
<1-65535>	Specify the actual label value.
lt	Indicate the lt keyword, which specifies a destination port as less than a given value.
<0-65535>	Specify the actual less than value.
log	Log the results.
ne	Indicate the ne keyword, which specifies a destination port as not equal to a given value.
<0-65535>	Specify the actual not equal than value.
pkt-size	Indicate the packet keyword, which is used to identify packet size.
gt	Packet size less than or greater than specified value.
lt	Packet size less than or greater than specified value.
range	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
<0-65535>	Specify the actual range of values for packet size from <0-65535>.
precedence	Indicate the precedence keyword, which is used to identify a packet filter precedence level.
<0-7>	Specify the precedence value.
tos	Type of Service (ToS) value; also used to filter packets.
<0-255>	Specify the actual value for ToS.
range	Indicate the range keyword.
<0-255>	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#ipv6 access-list zebos TK deny tcp 2::2/64 eq 14 3::4/64 lt 12 log
```

ipv6 access-list zebos udp

Use this command to configure an access list for filtering frames that permit or deny multiple IANA protocols. An access list controls the transmission of packets on an interface, and restrict the content of routing updates. The switch stops checking the access list when a match is encountered.

Some protocols are identified by name, such as IP, GRE, or TCP packets. Other are identified by a number in the range of <0-255>. Use mask to specify a subset of addresses. Use `any` to allow all packets.

Use the `no` option with any of the `access-list zebos` command variants to remove a specified access-list.

Command Syntax

```
ipv6 access-list zebos WORD (deny|permit) (udp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|) ({label <1-
  65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size ((lt|gt)
  <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out) IFNAME}|)

no ipv6 access-list zebos WORD (deny|permit) (udp) (X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>|)
  ({label <1-65535>|precedence <0-7>|tos (<0-255>| range <0-255> <0-255>)|pkt-size
  ((lt|gt) <0-65535>|range <0-65535> <0-65535>)|fragments|log|interface (in|out)
  IFNAME}|)
```

Parameters

`WORD`	Access-list name.
`deny`	Specify route to deny.
`permit`	Specify route to permit.
`udp`	Specify User Datagram Protocol packet.
`X:X::X:X`	Source IP address.
`X:X::X:X/M`	Source IP address and mask.
`any`	Source any local address.
`X:X::X:X`	Destination IP address.
`X:X::X:X/M`	Destination IP address and mask.
`any`	Destination any local address.
`eq`	Indicate the `eq` keyword, which specifies a source port as equal to a given value.
`<0-65535>`	Specify the actual equal to value.
`gt`	Indicate the `gt` keyword, which specifies a source port as greater than a given value.
`<0-65535>`	Specify the actual greater than value.
`lt`	Indicate the `lt` keyword, which specifies a source port as less than a given value.
`<0-65535>`	Specify the actual less than value.
`ne`	Indicate the `gt` keyword, which specifies a source port as not equal to a given value.
`<0-65535>`	Specify the actual not equal to value.
`range`	Indicate the `range` keyword, which is used to specify the range of a source port.
`<0-255>`	Specify the actual range of the source port from <0 to 255>.

`eq`	Indicate the `eq` keyword, which specifies a destination port as equal to a given value.
`<0-65535>`	Specify the actual equal to value.
`fragments`	Indicate the `fragments` keyword. An ACL applies to the non-initial fragment of packet.
`gt`	Indicate the `gt` keyword, which specifies a destination port as greater than a given value.
`<0-65535>`	Specify the actual greater than value.
`interface`	Indicate the `interface` keyword, which is the name of the input or output interface.
`in`	Specify the actual input interface.
`out`	Specify the actual output interface.
`IFNAME`	Specify the actual interface name.
`label`	Indicate the `label` keyword, which is used to identify an application.
`<1-65535>`	Specify the actual label value.
`log`	Log the results.
`lt`	Indicate the `lt` keyword, which specifies a destination port as less than a given value.
`<0-65535>`	Specify the actual less than value.
`ne`	Indicate the `ne` keyword, which specifies a destination port as less than a given value.
`<0-65535>`	Specify the actual not equal than value.
`pkt-size`	Indicate the `packet` keyword, which is used to identify packet size.
`gt`	Packet size less than or greater than specified value.
`lt`	Packet size less than or greater than specified value.
`range`	A range of type of service values. The first value is the beginning of the range and the second value is the end of the range.
`<0-65535>`	Specify the actual range of values for packet size from <0-65535>.
`precedence`	Indicate the `precedence` keyword, which identifies a packet filter precedence level.
`<0-7>`	Specify the precedence value.
`range`	Indicate the `range` keyword, which is used to specify the range of a destination port.
`<0-255>`	Specify the actual range of the destination port from <0 to 255>.
`tos`	Type of service (ToS) value; also used to filter packets.
`<0-255>`	Specify the actual value for ToS.
`range`	Indicate the `range` keyword.
`<0-255>`	Specify the actual range of values for ToS from <0 to 255>.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#ipv6 access-list zebos TK deny udp 2::2/64 eq 14 3::4/64 lt 12 log
```

ipv6 mroute

Use this command to create a multicast static route. Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform RPF checks. Use the `no` form of this command to clear the route.

Command Syntax

```
ipv6 mroute X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE
ipv6 mroute X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)
ipv6 mroute X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE <1-255>
ipv6 mroute X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE) <1-255>
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE
  <1-255>
ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)
  <1-255>
no ipv6 mroute X:X::X:X/M static|rip|ospf|bgp|isis|)
no ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|)
```

Parameters

`vrf`	Specify the VRF name for the static route.
`X:X::X:X/M`	Specify multicast source IP address and mask
`X:X::X:X`	RPF address for the multicast route. Host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up one level.
`INTERFACE`	Incoming interface name. Can only be specified for non-broadcast interfaces.
`bgp`	Specify the border gateway protocol (BGP).
`isis`	Specify the Intermediate system to intermediate system (IS-IS) protocol.
`ospf`	Specify the open shortest patch first (OSPF) protocol.
`rip`	Specify the routing information protocol (RIP) protocol.
`static`	Specify Static routes.
`X:X::X:X`	Specify Reverse path forwarding (RPF) neighbor address or route.
`INTERFACE`	Specify Reverse path forwarding (RPF) interface or pseudo interface.
`<1-255>`	Specify whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. Default is 0.

Command Mode

Configure mode

Example

```
(config)#ipv6 mroute 10:10::10:50/1 255.255.255.0 1
```

log file

Use this command to specify the log file controls and where to save the logs in a configuration file. This command enables writing of debug output to the disk file. If not specified, the system uses a default filename. The default directory for all VR log files is `/var/local/zebos/log/<vr-name>`. Log output can also be written to default log file, which is usually `usr/local/sbin`.

Use option no to cancel writing to a specific log file.

Command Syntax

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

Parameter

`FILENAME`	Specify the name of the log file.

Command Mode

Configure mode

Examples

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

```
#configure terminal
(config)#log file /usr/local/sbin/bgpd.log
(config)#log file /var/local/zebos/log/vrname
```

log syslog

Use this command to begin logging of information to the system log and set the level to debug.

Syslog enables centrally logging and analyzing of configuration events and system error messages. This helps monitor interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug sessions. The command instructs the `VLOGD` daemon to forward all PVR debug output from all active `terminal monitor` sessions to the syslog file.

Use the `no` parameter to disable logging to the system log.

Command Syntax

```
log syslog
no log syslog
```

Parameters

None

Command Mode

Configure mode

Example

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

mac-access-list

Use the `mac` command to configure a MAC access list.

Use the `no` parameter to remove this configuration.

Command Syntax

```
mac-access-list <2000-2699> (deny|permit) MAC MASK MAC MASK <1-8>
mac-access-list <2000-2699> (deny|permit) MAC MASK any <1-8>
mac-access-list <2000-2699> (deny|permit) any MAC MASK <1-8>
mac-access-list <2000-2699> (deny|permit) MAC MASK MAC MASK <1-8>
mac-access-list <2000-2699> (deny|permit) MAC MASK any <1-8>
mac-access-list <2000-2699> (deny|permit) any MAC MASK <1-8>
```

Parameters

`<2000-2699>`	Specify an extended MAC ACL.
`deny`	Specify packets to reject.
`permit`	Specify packets to permit.
`MAC`	Specify a source MAC address in HHHH.HHHH.HHHH format for a host.
`MASK`	Specify a source wildcard in HHHH.HHHH.HHHH format.
`any`	Specify a source as any.
`MAC`	Specify a destination MAC address in HHHH.HHHH.HHHH format for a host.
`MASK`	Specify a destination wildcard in HHHH.HHHH.HHHH format.
`<1-8>`	Specify the format for a packet (for example, 1:Ethernet II/ 2:802.3/ 4:SNMP/ 8:LLC).

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#mac-access-list 2000 deny any 1111.1111.1111 1 1
```

maximum-access-list

Use this command to set the maximum number of access-list entries.

Use the `no` parameter to disable this command.

Command Syntax

```
maximum-access-list <1-4294967294>
no maximum-access-list
```

Parameters

`<1-4294967294>` Specify the maximum number of access lists.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#maximum-access-list 123

(config)#no maximum-access-list
```

router-id

Use this command to add a router identifier for this system.

Use the `no` form of this command to disable this function.

Command Syntax

```
router-id A.B.C.D
no router-id (A.B.C.D|)
```

Parameters

`A.B.C.D`	Specifies the router identifier in IP address format for this system.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#router-id 123.12.3.123
(config)#
```

service password-encryption

Use this command to specify encryption of passwords. Encryption helps prevent observers from reading passwords.

Note: When using the `service password-encryption` command through IMISH, you must write to memory using the `write memory` or `write file` command. If you have not written to memory, the change made by this command (encryption) is not available when you log into IMISH the next time. See write on page 62 for more information.

Use the `no` parameter to disable this feature.

Note: Password can be an alpha-numeric string up to 80-characters, including spaces. The string cannot begin with a number.

Command Syntax

```
service password-encryption
no service password-encryption
```

Parameters

None

Command Mode

Configure mode

Example

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

service terminal-length

Use this command to set the terminal length for VTY sessions.

Use the `no` parameter to disable this feature.

Command Syntax

```
service terminal-length <0-512>
no service terminal-length (<0-512>|)
```

Parameters

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

Command Mode

Configure mode

Example

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

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

show arp

Use this command to display ARP (address resolution protocol) information for an interface.

Command Syntax

```
show arp
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

```
#show arp
Address           HWaddress              Interface      Type
10.1.2.1          a8:b1:d4:33:41:40       eth0          Dynamic
```

show router-id

Use this command to display the Router ID of the current system.

Command Syntax

```
show router-id
```

Parameters

None

Command Mode

Privileged Exec mode

Example

```
#show router-id
Router ID: 10.55.0.2 (automatic)
```

show running-config router-id

Use this command to show the running system global router ID configuration.

Command Syntax

```
show running-config router-id
```

Parameters

None

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config router-id
!
router-id 3.3.3.3
!
```

snmp restart nsm

Use this command to restart SNMP in Network Service Module (NSM)

Command Syntax

```
snmp restart nsm
```

Parameters

None

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#snmp restart nsm
```

CHAPTER 4 Common Router-map Mode Commands

This chapter provides an alphabetized reference for all Router-map mode commands. Commands are common to multiple NSM protocols. Unlike the Router mode, the Route-map mode is a general configuration mode and not specific to a particular protocol module.

This chapter includes the following commands:

match as-path

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

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

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove a path list entry.

Command Syntax

```
match as-path WORD
no match as-path (WORD|)
```

Parameter

`WORD`	Specify an autonomous system path access list name.

Default

Enabled

Command Mode

Route-map mode

Example

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

match community

Use this command to specify the community to be matched.

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

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

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove the community list entry.

Command Syntax

```
match community (<1-99>|<100-500>|WORD) (exact-match|)
no match community (<1-99>|<100-500>|WORD|) (exact-match|)
```

Parameters

`<1-99>`	Specify the community-list number (standard).
`<100-500>`	Specify the community-list number (expanded).
`WORD`	Specify the community-list name.
`exact-match`	Do exact matching of communities.

Command Mode

Route-map mode

Examples

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

match extcommunity

Use this command to match BGP external community list

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

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

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove the community list entry.

Command Syntax

```
match extcommunity (<1-99>|<100-500>|WORD) (exact-match|)
no match extcommunity (<1-99>|<100-500>|WORD|) (exact-match|)
```

Parameters

`<1-99>`	Specify the community-list number (standard).
`<100-500>`	Specify the community-list number (expanded).
`WORD`	Name of the community-list.
`exact-match`	Do exact matching of communities.

Command Mode

Route-map mode

Example

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

match interface

Use this command to define the interface match criterion. This command specifies the next-hop interface name of a route to be matched.

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

Command Syntax

```
match interface IFNAME
no match interface (IFNAME|)
```

Parameter

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

Default

Disabled

Command Mode

Route-map mode

Example

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

match ip address

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

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

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

Command Syntax

```
match ip address (<1-199>|<1300-2699>|WORD)
no match ip address (<1-199>|<1300-2699>|WORD|)
```

Parameters

`WORD`	Specify the IP access-list name.
`<1-199>`	Specify the IP access-list number (standard range).
`<1300-2699>`	Specify the IP access-list number (expanded range).

Command Mode

Route-map mode

Example

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

match ip address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command too disable this function

Command Syntax

```
match ip address prefix-list WORD
no match ip address prefix-list (WORD|)
```

Parameter

`WORD`	Specify the IP prefix list name.

Command Mode

Route-map mode

Examples

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

match ip next-hop

Use this command to specify a next-hop address to be matched in a route-map. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
match ip next-hop (<1-199>|<1300-2699>|WORD)
no match ip next-hop (<1-199>|<1300-2699>|WORD|)
```

Parameters

`WORD`	Specify the IP access-list name.
`<1-199>`	Specify the IP access-list number (standard range).
`<1300-2699>`	Specify the IP access-list number (expanded range).

Command Mode

Route-map mode

Examples

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

match ip next-hop prefix-list

Use this command to specify the next-hop IP address match criterion using the prefix-list. This command matches the next-hop IP address of a route.

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

Command Syntax

```
match ip next-hop prefix-list WORD
no match ip next-hop prefix-list (WORD|)
```

Parameter

`WORD`	A string specifying the prefix-list name.

Default

Disabled

Command Mode

Route-map mode

Examples

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

match ip peer

Use this command to specify the match peer IPv4 address of a route.

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

Command Syntax

```
match ip peer (<1-199>|<1300-2699>|WORD)
no match ip peer (<1-199>|<1300-2699>|WORD|)
```

Parameter

`WORD`	Specify the IP access-list name.
`<1-199>`	Specify the IP access-list number (standard range).
`<1300-2699>`	Specify the IP access-list number (expanded range).

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip peer 123

(config-route-map)#no match ip peer 123
```

match ipv6 address

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

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

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

Command Syntax

```
match ipv6 address WORD
no match ipv6 address (WORD|)
```

Parameter

`WORD`	Specify the IPv6 access list name.

Default

Disabled

Command Mode

Route-map mode

Examples

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

match ipv6 address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
match ipv6 address prefix-list WORD
no match ipv6 address prefix-list (WORD|)
```

Parameter

`WORD`	Specify the IPv6 access list name.

Command Mode

Route-map mode

Examples

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

match ipv6 next-hop

Use this command to specify the next-hop address to be matched. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

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

Use the `no` parameter with this command to disable this function

Command Syntax

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

Parameters

`X:X::X:X`	Specify the IPv6 address of the next-hop.
`WORD`	Specify the IPv6 access list name.

Command Mode

Route-map mode

Examples

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

match ipv6 next-hop prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
match ipv6 next-hop prefix-list WORD
no match ipv6 next-hop prefix-list WORD
```

Parameters

`WORD`	Specify the IPv6 access list name.

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 next-hop prefix-list new
```

match ipv6 peer

Use this command to specify the match peer IPv6 address of a route.

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

Command Syntax

```
match ipv6 peer (<1-199>|<1300-2699>|WORD)
no match ipv6 peer (<1-199>|<1300-2699>|WORD|)
```

Parameter

`WORD`	Specify the IP access-list name.
`<1-199>`	Specify the IP access-list number (standard range).
`<1300-2699>`	Specify the IP access-list number (expanded range).

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ipv6 peer 123

(config-route-map)#no match ipv6 peer 123
```

match metric

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

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
match metric <0-4294967295>
no match metric (<0-4294967295>|)
```

Parameters

`<0-4294967295>` Specify the metric value.

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match metric 888999
```

match origin

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

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

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

Note: This command is valid only for BGP.

Use the `no` parameter with this command to disable this matching.

Command Syntax

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

Parameters

`egp`	Remote exterior gateway protocol.
`igp`	Local internal gateway protocol.
`incomplete`	Unknown heritage.

Command Mode

Route-map mode

Example

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

match route-type

Use this command to match specified external route type. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes and external type-2 matches only Type 2 external routes.

Use the `no` parameter with this command to turn off the matching.

Command Syntax

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

Parameters

`type-1`	Match OSPF External Type 1 metric.
`type-2`	Match OSPF External Type 2 metric.

Default

Disabled

Command Mode

Route-map mode

Examples

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

match tag

Use this command to match the specified tag value.

Use the `no` parameter with this command to turn off the declaration.

Command Syntax

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

Parameters

`<0-4294967295>` Tag value.

Default

Disabled

Command Mode

Route-map mode

Examples

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

route-map

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

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

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

Use the `no` parameter with this command to turn off the declaration.

Note: Password can be an alpha-numeric string up to 80-characters, including spaces. The string cannot begin with a number.

Command Syntax

```
route-map WORD (deny|permit) <1-65535>
no route-map WORD ((deny|permit) <1-65535>|)
```

Parameters

`WORD`	Identify the route.
`deny`	Route map denies set operations. If the `deny` parameter is specified, and the match criteria are met, the route is not redistributed, and any other route maps with the same map tag are not examined.
`permit`	Route map permits set operations. If the `permit` parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the `match` criteria are not met, the next route map with the same tag is tested.
`<1-65535>`	Sequence to insert to or delete from an existing route-map entry.

Command Mode

Configure mode

Example

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

```
#configure terminal
(config)#route-map route1 permit 1
(config-route-map)#
```

set aggregator

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

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

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
set aggregator as <1-4294967295> A.B.C.D
no set aggregator as (<1-4294967295> A.B.C.D|)
```

Parameters

`as`	AS number of aggregator.
`<1-4294967295>`	Specify the AS number of aggregator.
`A.B.C.D`	Specify the IP address of aggregator.

Command Mode

Route-map mode

Examples

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

set as-path

Use this command to modify an autonomous system path for a route. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use this command to prepend an AS path string to routes increasing the AS path length.

To use this command, you must first give the `match` and `set` commands configure the conditions for redistributing routes from one routing protocol to another:

- The `match` command specifies the match criteria under which redistribution is allowed for the current route-map.
- The `set` command specifies the set redistribution actions to be performed if the match criteria are met.

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

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set as-path prepend .<1-65535>
set as-path prepend .<1-4294967295>
no set as-path prepend (.<1-65535>|)
no set as-path prepend (.<1-4294967295>|)
```

Parameters

`<1-65535>`	ZebOS-XP prepends this number to the AS path.
`<1-4294967295>`	ZebOS-XP prepends this number to the AS path.

Command Mode

Route-map mode

Examples

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

set atomic-aggregate

Use this command to set an atomic aggregate attribute.

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

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
set atomic-aggregate
```

```
no set atomic-aggregate
```

Parameters

None

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set atomic-aggregate
```

set comm-list

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

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

Command Syntax

```
set comm-list (<1-99>|<100-500>|WORD) delete
no set comm-list (<1-99>|<100-500>|WORD) delete
```

Parameters

`<1-99>`	Standard community-list number.
`<100-500>`	Expanded community-list number.
`WORD`	Name of the community-list.
`delete`	Delete the community-list.

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map ipi permit 3
(config-route-map)#set comm-list 34 delete
```

set community

Use this command to set the communities attribute. and group destinations in a certain community, as well as apply routing decisions according to those communities.

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

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

Use the `no` parameter with this command to delete the entry.

Command Syntax

```
set community [<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]
  (additive|)
no set community [AA:NN|internet|local-AS|no-advertise|no-export] (additive|)
```

Parameters

`<1-65535>`	Community number
`AA:NN`	The community number in aa:nn format.
`internet`	Specify the Internet.
`local-AS`	Specify no sending outside the local AS (well-known community).
`no-advertise`	Specify no advertisement of this route to eBGP peers
`no-export`	Specify no advertisement of this route to any peer.
`none`	Removes the community attribute from the prefixes that pass the route-map.
`additive`	Adds to the existing community.

Command Mode

Route-map mode

Examples

The following examples show the use of the `set community` command with different parameters.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-export no-advertise

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-advertise

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community 10:01 23:34 12:14 no-export
```

set dampening

Use this command to enable route-flap dampening and set parameters. Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

Use the `no` parameter with this command to delete the entry.

Command Syntax

```
set dampening <1-45> <1-20000> <1-20000> <1-255> (<1-45>|)
no set dampening <1-45> <1-20000> <1-20000> <1-255> (<1-45>|)
```

Parameters

`<1-45>`	Specify the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes.
`<1-20000>`	Specify the reuse-limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750.
`<1-20000>`	Specify the suppress-limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000.
`<1-255>`	Specify the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes).
`<1-45>`	Specify the unreachability half-life time for penalty, in minutes. The default value is 15 minutes.

Command Mode

Route-map mode

Example

```
#configure terminal
(config)#route-map R1 permit 24
(config-route-map)#set dampening 20 333 534 30
```

set extcommunity

Use this command to set an extended community attribute.

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

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
set extcommunity rt .AA:NN (additive|)
set extcommunity soo .AA:NN
set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>
no set extcommunity rt (.AA:NN|) (additive|)
no set extcommunity soo (.AA:NN|)
no set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>
```

Parameters

`rt`	Specify the route target of the extended community.
`soo`	Specify the site-of-origin of the extended community.
`cost`	Specify the extended cost community.
`igp`	Compare IGP cost comparison.
`pre-bestpath`	Compare bestpath calculation.
`<0-255>`	Community ID.
`<0-4294967295>`	Cost range.
`additive`	Add to the exsisting community.
`ASN:NN`	VPN extended community

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 06:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 0.0.0.6:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 06:01
```

```
#configure terminal
(config-route-map)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 0.0.0.6:01
```

set ip next-hop

Use this command to set the specified next-hop value.

Use the `no` parameter with this command to turn off the setting.

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

Command Syntax

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

Parameter

`A.B.C.D`	Specify the IP address of the next-hop.
`peer-address`	Specify the peer address (for BGP only).

Default

Disabled

Command Mode

Route-map mode

Examples

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

set ipv6 next-hop

Use this command to set a next hop-address.

Use the `no` parameter with this command to delete an entry.

Note: This command is valid for BGP and OSPFv3 only.

Command Syntax

```
set ipv6 next-hop X:X::X:X
set ipv6 next-hop local X:X::X:X
no set ipv6 next-hop (X:X::X:X|)
no set ipv6 next-hop local (X:X::X:X|)
```

Parameters

`X:X::X:X`	Specify the global IPv6 address of nexthop.
`local`	Specify the IPv6 local address.

Default

Disabled

Command Mode

Route-map mode

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set ipv6 next-hop local fe80::203:47ff:fe97:66dc
```

set level

Use this command to set the IS-IS level to export a route.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set level (level-1|level-2|level-1-2)
no set level (level-1|level-2|level-1-2|)
```

Parameters

`level-1`	Export into a level-1 area.
`level-2`	Export into a level-2 sub-domain.
`level-1-2`	Export into level-1 and level-2.

Default

Disabled

Command Mode

Route-map mode

Examples

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

set local-preference

Use this command to set the BGP local preference path attribute.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set local-preference <0-4294967295>
no set local-preference (<0-4294967295>|)
```

Parameters

`<0-4294967295>` Specify the tag value for destination routing protocol.

Default

Disabled

Command Mode

Route-map mode

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set local-preference 12
```

set metric

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

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

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

Use the `no` parameter with this command to disable this function.

Command Syntax

```
set metric (<0-4294967295>|<+/-metric>)
no set metric (<0-4294967295>|<+/-metric>|)
```

Parameters

`<0-4294967295>`	Specify a metric value.
`<+/-metric>`	Adds or subtracts a metric.

Command Mode

Route-map mode

Examples

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

set metric-type

Use this command to set the metric type for the destination routing protocol. Select a type to be either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

Note: This command is for OSPF, OSPFv3, or IS-IS only.

Use the `no` parameter with this command to return to the default.

Command Syntax

```
set metric-type (internal|external)
set metric-type (type-1|type-2)
no set metric-type (internal|external|)
no set metric-type (type-1|type-2|)
```

Parameters

`external`	Specify an IS-IS external metric type.
`internal`	Specify an IS-IS internal metric type.
`type-1`	Specify an OSPF external type 1 metric.
`type-2`	Specify an OSPF external type 2 metric

Command Mode

Route-map mode

Example

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

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

set origin

Use this command to set the BGP origin code. The origin attribute defines the origin of the path information. The three parameters with this command indicate three different values. `IGP` is interior to the originating AS. This happens if IGP is redistributed into the BGP. `EGP` is learned through an Exterior Gateway Protocol. Incomplete is unknown or learned through some other means. This happens when static route is redistributed in BGP and the origin of the route is incomplete.

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

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

Use the `no` parameter with this command to delete an entry.

Command Syntax

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

Parameters

`egp`	Specify a remote EGP (Exterior Gateway Protocol) system.
`igp`	Specify a local IGP (Internal Gateway Protocol) system.
`incomplete`	Specify a system of unknown heritage.

Command Mode

Route-map mode

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set origin egp
```

set originator-id

Use this command to set the originator ID attribute.

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

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

Use the `no` parameter with this command to disable this function

Command Syntax

```
set originator-id A.B.C.D
no set originator-id (A.B.C.D|)
```

Parameter

`A.B.C.D`	Specify the IP address of originator.

Command Mode

Route-map mode

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set originator-id 1.1.1.1
```

set tag

Use this command to set a tag value. The parameter is the route tag that is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. In addition, when using route-map, ZebOS-XP can tag the LSAs with the appropriate tag value. Sometimes the tag matches with using route-map, and sometimes, the value may be used by another application.

Use the `no` parameter with this command to return to the default.

Command Syntax

```
set tag <0-4294967295>
no set tag (<0-4294967295>|)
```

Parameter

`<0-4294967295>` Specify the tag value for destination routing protocol.

Command Mode

Route-map mode

Example

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

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

set vpnv4 next-hop

Use this command to set a VPNv4 next-hop address.

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

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

Note: This command is valid for BGP, only

Use the `no` parameter with this command to disable this function

Command Syntax

```
set vpnv4 next-hop A.B.C.D
no set vpnv4 next-hop (A.B.C.D|)
```

Parameter

`A.B.C.D`	Specifies the IP address of originator.

Command Mode

Route-map mode

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set vpnv4 next-hop 6.6.6.6
```

set weight

Use this command to set weights for the routing table.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

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

Note: This command is valid only for BGP.

Use the `no` parameter with this command to delete an entry.

Command Syntax

```
set weight <0-4294967295>
no set weight (<0-4294967295>|)
```

Parameter

`<0-4294967295>` Specify the weight value.

Command Mode

Route-map mode

Examples

In the following configuration, all routes that apply to access-list 10 will have the weight set at 400. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match as-path 10
(config-route-map)#set weight 400
```

show route-map

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

Command Syntax

```
show route-map (|WORD)
```

Parameters

WORD	Displays route-map information.

Command Mode

Exec mode and Privileged Exec mode

Example

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

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

show running-config route-map

Use this command to show the running system status and configuration details for route-map.

Command Syntax

```
show running-config route-map
```

Parameters

None

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config route-map
!
route-map abc deny 2
 match community 2
!
route-map abc permit 3
 match route-type external type-2
 set metric-type type-1
!
```

CHAPTER 5 Interface Commands

This chapter provides an alphabetized reference for each of the interface CLI commands. It includes the following commands:

admin-group

Use this command to create an administrative group to be used for links. Each link can be a member of one or more, or no administrative groups.

When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. There can be multiple groups per interface. The group is created in the Configure mode, then interfaces are added to the group in the Interface mode.

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

Note: This command is unavailable if you are running `imish`.

Command Syntax

```
admin-group NAME
```

```
no admin-group NAME
```

Parameters

`NAME`	Specify the name of the admin group to be added.

Command Mode

Interface mode

Example

In the following example, the `eth0` interface is added to the group `ipi`:

```
#configure terminal
(config)#interface eth0
(config-if)#admin-group ipi
```

clear counters

Use this command to clear the uRPF statistics on the interface for IPv4/IPv6Use the `no` parameter to remove the maximum bandwidth.

Command Syntax

```
clear counters <IFNAME>
```

Parameter

`IFNAME`	Name of the Interface.

Command Mode

Exec mode

Example

```
#clear counters eth2
```

bandwidth

Use this command to specify the maximum bandwidth to be used for each interface. The bandwidth value is in bits, and can also accept units.

Use the `no` parameter to remove the maximum bandwidth.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

Parameter

`BANDWIDTH`	Specify either `k` or `m` for 1 to 999 kilobits or megabits. Specify `g` for 1 to 10 gigabits.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#bandwidth 100m
```

clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv4 interface.

Command Syntax

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

Parameters

WORD	Specify the name of the prefix-list.
A.B.C.D/M	IP prefix and length.

Command Mode

Configure mode

Example

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

clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

Command Syntax

```
clear ipv6 neighbors
```

Parameters

None

Command Mode

Privileged Exec mode

Example

```
#clear ipv6 neighbors
```

clear ipv6 prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv6 interface.

Command Syntax

```
clear ipv6 prefix-list
clear ipv6 prefix-list WORD
clear ipv6 prefix-list WORD X:X::X:X/M
```

Parameters

WORD	Specify the name of the prefix-list.
X:X::X:X/M	IP prefix and length.

Command Mode

Configure mode

Example

```
#clear ipv6 prefix-list List1
```

description

Use this command to assign an description to an interface.

Use the `no` parameter to remove an interface description.

Command Syntax

```
description LINE
no description
```

Parameter

`LINE`	Interface description.

Command Mode

Interface mode

Examples

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

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

duplex

Use this command to set the duplex mode for each interface.

Use the `no` parameter to remove the duplex mode.

Command Syntax

```
duplex (half|full|auto)
no duplex
```

Parameter

`half`	Set the interface to half-duplex.
`full`	Set the interface to full-duplex.
`auto`	Set the interface to auto-negotiate.

Command Mode

Interface mode

Examples

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

(config-if)#no duplex
```

if-arbiter

Use this command to discover new interfaces recently added to the kernel and add them to the ZebOS-XP database.

This command starts the arbiter to check interface information periodically. ZebOS-XP dynamically finds any new interfaces added to the kernel. If an interface is loaded dynamically into the kernel when ZebOS-XP is already running, this command polls and updates the kernel information periodically.

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

Command syntax

```
if-arbiter (interval <1-65535>|)
no if-arbiter
```

Parameter

`interval`	Specify the interval (in seconds) after which NSM sends a query to the kernel.

Default

By default, `if-arbiter` is disabled. When interface-related operations are performed outside of ZebOS-XP (such as when using the `ifconfig` command), enable `if-arbiter` for a transient time to complete synchronization. When synchronization is complete, disable it by giving the `if-arbiter` command.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#if-arbiter interval 5
```

interface

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

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
interface IFNAME
no interface IFNAME
```

Parameter

`IFNAME`	Specify the name of the interface.

Command Mode

Configure mode

Example

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

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

ip access-group

Use this command to set the access-group for an interface. This command configures an access list to filter incoming, outgoing, or forwarded packets.

Use the no parameter with this command to disable the IP access group.

Command Syntax

```
ip access-group WORD (in|out|forward)
no ip access-group WORD (in|out|forward)
```

Parameters

WORD	Specify an access list name.
in	Specify to filter incoming packets.
out	Specify to filter outgoing packets.
forward	Specify to filter forwarded packets.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#access-list 1 permit 225.2.2.2 0.0.0.0
(config)#interface eth2
(config-if)#ip access-group 1 forward

(config)#interface eth2
(config-if)#no ip access-group 1 forward
```

ip address A.B.C.D/M

Use this command to specify that an IP address and prefix length will be used by this interface. If the `secondary` parameter is not specified, this command overwrites the primary IP address. If the `secondary` parameter is specified, this command adds a new IP address to the interface. The secondary address cannot be configured in the absence of a primary IP address. The primary address cannot be removed when a secondary address is present.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address A.B.C.D/M (label) LINE
ip address A.B.C.D/M (secondary|)
ip address A.B.C.D/M (secondary) (label) LINE
no ip address A.B.C.D/M label LINE
no ip address A.B.C.D/M secondary label LINE
no ip address (A.B.C.D/M (secondary|)|)
```

Parameters

`label`	Specify the label of this address.
`LINE`	Specify the actual label.
`secondary`	Specify the IP address as secondary.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
```

ip address DHCP

Use this command to specify that a DHCP client will be used to obtain an IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
(config-if)#ip address dhcp
```

ip forwarding

Use this command to turn on IP forwarding.

Use the `no` parameter with this command to turn off IP forwarding.

Command Syntax

```
ip forwarding
no ip forwarding
```

Parameters

None

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ip forwarding
```

ip policy route-map

Use this command to enable PBR on an interface for a given route-map

Use `no` parameter with this command to disable PBR on an interface for a given route map.

Command Syntax

```
ip policy route-map WORD
no ip policy route-map WORD
```

Parameter

`WORD`	Specifies name of the route-map.

Command Mode

Interface mode

Example

In the following configuration example is used to forward packets to different routes based on the source IP address:

```
(config)#interface eth0
(config-if)#ip address 172.1.2.1 255.255.255.0
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 172.1.1.1 255.255.255.0
(config-if)#ip policy route-map policy_1
(config-if)#exit
(config)#access-list 10 permit ip host 172.1.1.10 any
(config)#access-list 11 permit ip host 172.1.1.11 any
(config)#route-map policy_1 permit 10
(config-route-map)#match ip address 10
(config-route-map)#set ip next-hop 172.1.2.10
(config-route-map)#exit
(config)#route-map policy_1 permit 11
(config-route-map)#match ip address 11
(config-route-map)#set ip next-hop 172.1.2.11
```

ip prefix-list

Use this command to create an entry for a prefix list.

A router starts to match prefixes from the top of the prefix list and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5. Use the parameters `GE` and `LE` specify the range of the prefix length to be matched. When setting these parameters, set `LE` to be less than 32 and `GE` to be less than `LE` value.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ip prefix-list WORD (deny|permit) (A.B.C.D/M|any)
ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32>
ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
no ip prefix-list WORD
no ip prefix-list WORD (deny|permit) (A.B.C.D/M|any)
no ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32>
no ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-
  32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-
  32>
ip prefix-list sequence-number
no ip prefix-list sequence-number
ip prefix-list WORD description LINE
no ip prefix-list WORD description LINE
no ip prefix-list WORD description
```

Parameters

WORD	Specify the name of a prefix list.
deny	Specify that packets are to be rejected.
description	Prefix-list specific description.
LINE	Up to 80 characters describing this prefix-list
permit	Specify that packets are to be accepted.
A.B.C.D/M	The IP address mask and length of the prefix list mask (A.B.C.D/M).
le	Maximum prefix length to be matched <0-32>.
ge	Minimum prefix length to be matched <0-32>.
seq	The sequence number of the prefix list <1-429496725>.
any	Takes all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for IPPREFIX.
sequence-number	Include and exclude sequence numbers in nonvolatile generation (NVGEN).

Command Mode

Configure mode

Examples

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

```
#conf t
(config)#router bgp 100
(config-router)#network 172.1.1.0
(config-router)#network 172.1.2.0
(config-router)#
(config-router)#neighbor 10.6.5.3 remote-as 300
(config-router)#neighbor 10.6.5.3 prefix-list mylist out
(config-router)#exit
(config)#ip prefix-list mylist seq 5 deny 76.2.2.0/24
(config)#ip prefix-list mylist seq 10 permit 0.0.0.0/0
```

ip proxy-arp

Use this command to enable the proxy ARP feature on an interface.

Use the `no` parameter to disable the proxy ARP feature on an interface.

Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

Parameters

None

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip proxy-arp
```

ip remote-address

Use this command to set the remote address (far end) on a point-to-point non multi-access link. This command can be used only on unnumbered interfaces. When a new remote-address is configured, the old address gets overwritten.

Use the `no` parameter to disable this function.

Command Syntax

```
ip remote-address A.B.C.D/M
no ip remote-address
```

Parameter

`A.B.C.D/M`	IP address and prefix length of the link remote address.

Command Mode

Interface mode

Example

```
(config)#interface ppp0
(config-if)#ip unnumbered eth1
(config-if)#ip remote-address 1.1.1.1/32
```

ip unnumbered

Use this command to enable IP processing without an explicit address on a point-to-point non multi-access link. Moreover, this command lets an interface borrow the IP address of a specified interface to enable IP processing on a point-to-point interface without assigning it an explicit IP address. In this way, the IP unnumbered interface can borrow the IP address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to unconfigure this feature on an interface.

Command Syntax

```
ip unnumbered IFNAME
no ip unnumbered
```

Parameter

`IFNAME`	A string that specifies the interface.

Command Mode

Interface mode

Examples

The following example creates a tunnel on Router 1 (eth1).

On Router 1

```
(config)#interface lo
(config-if)#ip address 127.0.0.1/8
(config-if)#ip address 33.33.33.33/32 secondary
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 10.10.10.145/24
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode gre
(config-if)#ip unnumbered eth1
(config-if)#exit
(config)#router ospf
(config-router)#network 10.10.10.0/24 area 0
```

ip vrf forwarding

This command associates an interface with a VRF.

Use the `no` parameter with this command to unbind an interface.

Command Syntax

```
ip vrf forwarding WORD
no ip vrf forwarding WORD
```

Parameter

`WORD`	Name of the VRF created using the ip vrf command in the configure mode (see ip vrf forwarding on page 167 command).

Command Mode

Interface mode

Example

```
#configure terminal
(config)#ip vrf IPI
(config)#interface eth1
(config-if)#ip vrf forwarding IPI
```

Note: When you give the `ip vrf forwarding` command within the Interface Configuration or Subinterface Configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. After giving the command, the IP attributes must then be configured in the context of the VRF.

ipv6 address

Use this command to set the IPv6 address of an interface.

Use the `no` form of this command to disable this function.

Command Syntax

```
ipv6 address X:X::X:X/M
ipv6 address X:X::X:X/M anycast
no ipv6 address X:X::X:X/M
```

Parameters

`X:X::X:X/M`	Specify the IP destination prefix and a mask length <0-128>.
`anycast`	Specify the anycast flag.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 address 3ffe:506::1/64
```

ipv6 forwarding

Use this command to turn on IPv6 forwarding.

Use the `no` parameter with this command to turn off IPv6 forwarding.

Command Syntax

```
ipv6 forwarding
```

```
no ipv6 forwarding
```

Parameters

None

Command Mode

Command mode

Example

```
#configure terminal
(config)#ipv6 forwarding
```

ipv6 nd current-hoplimit

Use this command to set an ND (Neighbor Discovery) advertised hop limit for an interface.

Use the `no` option with the command to remove the current hop limit.

Command Syntax

```
ipv6 nd current-hoplimit <0-255>
no ipv6 nd current-hoplimit (<0-255>|)
```

Parameter

`<0-255>`	Set a hop limit within this range.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd current-hoplimit 10
(config-if)#no ipv6 nd current-hoplimit
```

ipv6 nd link-mtu

Use this command to set an advertised MTU option.

Use the `no` option with the command to reset the MTU option to the default statute.

Command Syntax

```
ipv6 nd link-mtu (<1280-65535>)
no ipv6 nd link-mtu
```

Parameters

`<1280-65535>`	Set a link MTU value within this range.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd link-mtu 1600
(config-if)#no ipv6 nd link-mtu
```

ipv6 nd managed-config-flag

Use this command to set the managed address configuration flag in the Router Advertisement to be used for the IPv6 address auto-configuration.

Use the `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Parameters

None

Default

Unset

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd managed-config-flag
(config-if)#no ipv6 nd managed-config-flag
```

ipv6 nd minimum-ra-interval

Use this command to set a minimum Router Advertisement (RA) interval for the interface.

Use the `no` option with the command to remove the minimum RA interval.

Command Syntax

```
ipv6 nd minimum-ra-interval <3-1350>
no ipv6 nd minimum-ra-interval (<3-1350>|)
```

Parameter

`<3-1350>`	Minimum router advertisement interval (in seconds).

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd minimum-ra-interval 400
(config-if)#no ipv6 nd minimum-ra-interval
```

ipv6 nd other-config-flag

Use this command to set the other stateful configuration flag in Router Advertisement to be used for IPv6 address auto-configuration.

Use `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Parameters

None

Default

Unset

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd other-config-flag
(config-if)#no ipv6 nd other-config-flag
```

ipv6 nd prefix

Use this command to specify the IPv6 prefix information that is advertised by the Router Advertisement for IPv6 address auto-configuration.

Use `no` parameter with this command to reset the IPv6 prefix.

Command Syntax

```
ipv6 nd prefix X:X::X:X/M <0-4294967295> <0-4294967295> (off-link|) (no-
  autoconfig|)
ipv6 nd prefix X:X::X:X/M
ipv6 nd prefix valid-lifetime <0-4294967295>
ipv6 nd prefix preferred-lifetime <0-4294967295>
ipv6 nd prefix offlink
ipv6 nd prefix no-autoconf
no ipv6 nd prefix X:X::X:X/M
no ipv6 nd prefix valid-lifetime (<0-4294967295>|)
no ipv6 nd prefix preferred-lifetime (<0-4294967295>|)
no ipv6 nd prefix offlink
no ipv6 nd prefix no-autoconf
```

Parameters

`X:X::X:X/M`	Specify the IPv6 prefix.
`<0-4294967295>`	Range of values for valid lifetime in seconds.
`no-autoconfig`	Specify the IPv6 prefix no autoconfiguration flag.
`off-link`	Specify the IPv6 prefix off-link flag.
`preferred-lifetime`	Specify the IPv6 prefix preferred lifetime.
`<0-4294967295>`	Range of values for preferred lifetime in seconds.
`valid-lifetime`	Specify theIPv6 prefix valid lifetime <0-4294967295>.
`<0-4294967295>`	Range of values for valid lifetime in seconds.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#ipv6 nd prefix 2001:ffff::/64

(config)#interface eth0
(config-if)#ipv6 nd prefix no-autoconf

(config)#interface eth0
(config-if)#ipv6 nd prefix preferred-lifetime 550000
```

ipv6 nd ra-interval

Use this command to specify the interval between IPv6 Router Advertisements (RA).

Use `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd ra-interval <4-1800>
no ipv6 nd ra-interval
```

Parameter

`<4-1800>`	The RA interval in seconds.

Default

600 seconds

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd ra-interval 60
(config-if)#ipv6 nd prefix 3ffe:ffff:ffff::/64

(config-if)#no ipv6 nd ra-interval
```

ipv6 nd ra-lifetime

Use this command to specify the Router Advertisement (RA) lifetime of this router enabling it to act as a default gateway for the network.

Use `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd ra-lifetime <0-9000>
no ipv6 nd ra-lifetime
```

Parameter

`<0-9000>`	The RA lifetime duration in milliseconds.

Default

1800 seconds

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd ra-lifetime 9000
(config-if)#no ipv6 nd ra-lifetime
```

ipv6 nd reachable-time

Use this command to specify the reachable time in the Router Advertisement to be used for detecting unreachability of the IPv6 neighbor.

Use the `no` parameter with this command to reset the value to default.

Command Syntax

```
ipv6 nd reachable-time <0-3600000>
no ipv6 nd reachable-time
```

Parameter

`<0-3600000>`	The reachable time in milliseconds.

Default

Zero (0) milliseconds

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd reachable-time 1800000
(config-if)#no ipv6 nd reachable-time
```

ipv6 nd retransmission-time

Use this command to establish an IPv6 advertised retransmission time for the current interface.

Use the `no` form of the command to remove the retransmission time.

Command Syntax

```
ipv6 nd retransmission-time <1000-3600000>
no ipv6 nd retransmission-time (<1000-3600000>|)
```

Parameter

`<1000-3600000>` The retransmission time in milliseconds

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd retransmission-time 1200
(config-if)#no ipv6 nd retransmission-time
```

ipv6 nd suppress-ra

Use this command to suppress IPv6 Router Advertisement (RA) transmission for the current interface. Router Advertisement is used for IPv6 stateless auto-configuration.

Use `no` parameter with this command to enable Router Advertisement transmission.

Command Syntax

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

Parameters

None

Default

Suppressed

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 nd suppress-ra
```

ipv6 neighbor

Use this command to add an IPv6 neighbor entry.

Use the `no` form of this command to an IPv6 neighbor entry.

Command Syntax

```
ipv6 neighbor X:X::X:X IFNAME MAC
no ipv6 neighbor X:X::X:X IFNAME
```

Parameters

`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`MAC`	Specify the MAC hardware address <HHHH.HHHH.HHHH>.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ipv6 neighbor 2000::3 eth1 0010.1842.3dc1
(config)#no ipv6 neighbor 2000::3 eth1
```

ipv6 prefix-list

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

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

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

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ipv6 prefix-list WORD (deny|permit) (X:X::X:X/M|any)
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128>
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128>
ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-
  128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-
  128>
no ipv6 prefix-list WORD
no ipv6 prefix-list WORD (deny|permit) (X:X::X:X/M|any)
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128>
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128>
no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le
  <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge
  <0-128>
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number
ipv6 prefix-list WORD description LINE
no ipv6 prefix-list WORD description
```

Parameters

`seq`	The sequence number of the prefix list <1-429496725>.
`WORD`	Specify the name of a prefix list.
`description`	Prefix-list specific description.
`LINE`	Up to 80 characters describing this prefix-list
`deny`	Specify that packets are to be rejected.
`permit`	Specify that packets are to be accepted.
`IPPREFIX`	The IP address mask and length of the prefix list mask (X:X::X:X/M).
`le`	Maximum prefix length to be matched <0-128>.
`ge`	Minimum prefix length to be matched <0-128>.
`any`	Takes all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for IPPREFIX.
`sequence-number`	Include and exclude sequence numbers in nonvolatile generation (NVGEN).

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ipv6 prefix-list mylist seq 12345 deny 3ffe:345::/16 le 22 ge 14
```

ipv6 unnumbered

Use this command to enable IPv6 processing without an explicit address, on a point-to-point non multi-access link.

This command lets an interface borrow the IPv6 address of a specified interface to enable IPv6 processing on a point-to-point interface without assigning it an explicit IPv6 address. In this way, the IPv6 unnumbered interface can borrow the IPv6 address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to unconfigure this feature on an interface.

Command Syntax

```
ipv6 unnumbered IFNAME
no ipv6 unnumbered
```

Parameter

`IFNAME`	A string that specifies the interface.

Command Mode

Interface mode

Example

The following example creates a tunnel on Router 1 (eth1):

On Router 1

```
#configure terminal
(config)#interface lo
(config-if)#ipv6 address::1/128
(config-if)#exit
(config)#interface eth1
(config-if)#ipv6 address fe80::20e:cff:fe6e:56dd/64
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode gre
(config-if)#ipv6 unnumbered eth1
(config-if)#ipv6 router ospf area 0 tag 1
(config-if)#exit
(config)#router ipv6 ospf 1
(config-router)#router-id 10.70.0.145
```

mtu

Use this command to set the Maximum Transmission Unit (MTU) size of an interface.

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

Command Syntax

```
mtu <68-16338>
no mtu
```

Parameter

`<68-16338>`	Specify the size of MTU in bytes. <68-16338> for L2 packet, <576-9216> for L3 IPv4 packet and <1280-9216> for L3 IPv6 packet.

Command Mode

Interface mode

Example

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

multicast

Use this command to set the multicast flag to an interface.

Use the `no` form of this command to disable this function.

Command Syntax

```
multicast
no multicast
```

Parameters

None

Command Mode

Interface mode

Example

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

show interface

Use this command to display interface configuration and status.

Command Syntax

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

Parameter

IFNAME	Displays the name of a specific interface for which status and configuration data is desired.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is what this command displays when the interface is added:

```
#show interface eth5
Interface eth5
scope: both
Hardware is Ethernet  Current HW addr: 0800.27ea.3cd1
Physical:0800.27ea.3cd1  Logical:(not set)
index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Speed 1g
DHCP client is disabled.
inet 10.12.4.111/24 broadcast 10.12.4.255
inet6 fe80::a00:27ff:feea:3cd1/64
Max-vport 4096
Virtual port bind allowed
input packets 1612, bytes 187627, dropped 0, multicast packets 71
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 59, bytes 7323, dropped 0 ,uRPF_dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0,
collisions 0
```

show ip access-list

Use this command to display a IP access lists.

Command Syntax

```
show ip access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
```

Parameters

`<1-99>`	Display an IP standard access list.
`<100-199>`	Display an IP extended access list.
`<1300-1999>`	Display an IP standard access list (expanded range).
`<2000-2699>`	Display an IP extended access list (expanded range).
`WORD`	Display an IP access-list name.

Command Mode

Exec mode and Privileged Exec mode

Example

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

```
#show ip access-list
Standard IP access list 13
    permit any
Standard IP access list 67
    deny 1.1.1.0, wildcard bits 0.0.0.255
Extended IP access list 134
    deny ip 1.1.1.0 0.0.0.255 any
ZebOS IP access list 1111
    deny 1.1.1.1/1 exact-match
Standard IP access list 1340
    deny 1.1.1.0, wildcard bits 0.0.0.255
Extended IP access list 2001
    deny ip 1.1.1.0 0.0.0.255 any
ZebOS extended IP access list TK
    deny   tcp 2.2.2.3/24 eq 14 3.3.3.4/24 lt 12 log
ZebOS IP access list mylist
    deny   10.10.0.72/24 exact-match
    permit any
ZebOS extended IP access list new
    deny   icmp any any
ZebOS extended IP access list tk
    deny   tcp 2.2.2.3/24 eq 14 3.3.3.4/24 lt 12 log
#
```

show ip forwarding

Use this command to display the IP forwarding status.

Command Syntax

```
show ip forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of the `show ip forwarding` command displaying the IP forwarding status.

```
#show ip forwarding
IP forwarding is on
#
```

show ip interface (IPv4)

Use this command to display brief information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

Command Syntax

```
show ip interface brief
show ip interface IFNAME brief
```

Parameters

`IFNAME`	Display the name of the interface.
`brief`	Brief summary of IP status and configuration.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output from the `show ip interface brief` command:

```
#show ip interface brief
Interface   IP-Address   Status    Protocol    GMPLS Type      RPF Type
lo         127.0.0.1     up          up       MPLS            None
p1p1       unassigned    up          up       MPLS            Strict
p1p2       unassigned    up         down      MPLS             None
em1        10.12.20.27   up          up       MPLS             None
svlan0.1   unassigned    up         down      MPLS             None
Labeled bytes      : 0/0/0/0/0
```

show ip interface (IPv6)

Use this command toshow the urpf configuration on the interface for IPv6. To display information about a specific interface, specify the interface name with the command.

Command Syntax

```
show ipv6 interface brief
```

Parameters

None.

Command Mode

Exec mode

Example

The following is a sample output from the `show ipv6 interface brief` command:

```
#show ipv6 interface brief
p8p1                  2002::1
                      3ffe::1                                          [admin
down/down]
p7p1                  100:4::2
                      2001::1
                      fe80::56dd
                      fe80::a00:27ff:fe18:847e                         [up/up]
p2p1                  100:3::2
                      2ffe::1
                      fe80::a00:27ff:fe5c:cb12                         [up/up]
lo                    ::1                                              [up/up]
```

show interface brief

Use this command to display status of both L2 and L3 (ALL) interfaces

Command Syntax

```
show interface brief <IFNAME|>
```

Parameters

brief	Brief summary of IP status and configuration.
IFNAME	Display the name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Example

```
tr3-1#show interface brief
 --------------------------------------------------------------------------------
Interface     Type             Status  Reason                 Speed
Interface
--------------------------------------------------------------------------------
eth0          Management Ethernet  up      --                     96k
--------------------------------------------------------------------------------
Ethernet     VLAN  Type        Mode        Status  Reason          Speed  Port
Interface                                                                Ch #
--------------------------------------------------------------------------------
ge1          --    Ethernet    routed      up      none            1g     --
ge2          --    Ethernet    routed      down    Protocol down   0      --
ge3          --    Ethernet    routed      up      none            1g     --
ge4          --    Ethernet    routed      up      none            1g     --
ge5          --    Ethernet    routed      down    Protocol down   0      --
ge6          --    Ethernet    routed      down    Protocol down   0      --
ge7          --    Ethernet    routed      down    Protocol down   0      --
ge8          --    Ethernet    routed      down    Protocol down   0      --
ge9          --    Ethernet    routed      down    Protocol down   0      --
ge10         --    Ethernet    routed      down    Protocol down   0      --
ge11         --    Ethernet    routed      down    Protocol down   0      --
ge12         --    Ethernet    routed      down    Protocol down   0      --
ge13         1     Ethernet    trunk       up      none            1g     --
--------------------------------------------------------------------------------
Interface    Status      Description
--------------------------------------------------------------------------------
lo           up          --


--------------------------------------------------------------------------------
Interface    Status   Reason
--------------------------------------------------------------------------------
vlan1.1      up       --
vlan1.2      down     Protocol down
vlan1.3      down     Protocol down
vlan1.4      down     Protocol down
vlan1.5      down     Protocol down
```

```
vlan1.6      down     Protocol down
vlan1.7      down     Protocol down
vlan1.8      down     Protocol down
vlan1.9      down     Protocol down
vlan1.10     down     Protocol down
xe1          --    Ethernet    routed      down    Protocol down  10g    --
xe2          --    Ethernet    routed      down    Protocol down  10g    --
xe3          --    Ethernet    routed      down    Protocol down  10g    --
xe4          --    Ethernet    routed      down    Protocol down  10g    --
```

show interface switchport brief

Use this command to display status of only L2 or switchport interfaces.

Command Syntax

```
show interface switchport brief
```

Parameters

`brief`	Brief summary of IP status and configuration.

Command Mode

Exec mode

Example

```
tr3-1#show interface switchport brief


--------------------------------------------------------------------------------
Ethernet     VLAN  Type        Mode        Status  Reason         Speed  Port
Interface                                                                Ch #
--------------------------------------------------------------------------------
ge13         1     Ethernet    trunk       up      none           1g     --
```

show ip route

Use this command to display the IP routing table for a protocol or from a particular table.

Command Syntax

```
show ip route A.B.C.D
show ip route A.B.C.D/M
show ip route (database|)
show ip route (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ip route summary
show ip route vrf WORD (database|)
show ip route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
```

Parameters

`A.B.C.D`	Display network in the IP routing table.
`A.B.C.D/M`	Display IP prefix <network>/<length>, for example, 35.0.0.0/8.
`bgp`	Display Border Gateway Protocol (BGP) information.
`connected`	Display connected information.
`database`	Display IPv6 routing table database information.
`isis`	Display ISO IS-IS information.
`kernel`	Display kernel information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`static`	Display static routes.
`summary`	Display a summary of all routes
`vrf`	Display routes from a VPN Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Examples

When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. All best routes are entered into the FIB and can be viewed using this command. To display all routes (selected and not selected), use the `show ip route database` command. The following show output for the best routes.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default
```

```
O       1.1.1.0/24 [110/20] via 2.2.2.1, eth2, 00:00:10
C       2.2.2.0/24 is directly connected, eth2
C       3.3.3.0/24 is directly connected, eth1
O IA    4.4.4.0/24 [110/21] via 2.2.2.1, eth2, 00:00:10
K       10.10.0.0/24 via 10.70.0.1, eth0
C       10.70.0.0/24 is directly connected, eth0
C       33.33.33.33/32 is directly connected, lo
C       127.0.0.0/8 is directly connected, lo
K       169.254.0.0/16 is directly connected, eth0
```

The following is the output of this command with the `ospf` parameter, which displays only the selected OPSF routes learned by NSM:

```
#show ip route ospf
O       1.1.1.0/24 [110/20] via 2.2.2.1, eth2, 00:00:44
O IA    4.4.4.0/24 [110/21] via 2.2.2.1, eth2, 00:00:44
#
```

The following is the output of this command with the `summary` parameter.

```
#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
RouteSourceNetworks
kernel1
connected5
ospf2
Total8
FIB2
```

The following is an output of this command displaying the database routes learned by NSM. This output shows selected as well as non elected routes.

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       > - selected route, * - FIB route, p - stale info
K    *> 0.0.0.0/0 via 10.1.2.1, eth0
C    *> 4.4.4.40/32 is directly connected, lo
C    *> 10.1.2.0/24 is directly connected, eth0
C    *> 23.0.0.0/8 is directly connected, eth4
C    *> 34.0.0.0/24 is directly connected, eth2
C    *> 80.0.0.0/24 is directly connected, eth2
C    *> 127.0.0.0/8 is directly connected, lo
K    *> 169.254.0.0/16 is directly connected, eth0
C    *> 192.168.23.0/24 is directly connected, eth4
```


show ip prefix-list

Use this command to display the prefix list entries for IPv4 interfaces.

Syntax Description

```
show ip prefix-list
show ip prefix-list WORD
show ip prefix-list WORD seq <1-4294967295>
show ip prefix-list WORD A.B.C.D/M
show ip prefix-list WORD A.B.C.D/M longer
show ip prefix-list WORD A.B.C.D/M first-match
show ip prefix-list summary
show ip prefix-list summary WORD
show ip prefix-list detail
show ip prefix-list detail WORD
```

Parameters

`WORD`	Name of a prefix list.
`A.B.C.D/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Lookup longer prefix.
`seq`	Sequence number of an entry.
`<1-4294967295>`	Actual sequence number.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Example

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

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

show ip vrf

This command shows the routing information of the VRF.

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameter

WORD	Displays a name used to identify a VRF.

Command Mode

Exec mode and Privileged Exec mode

Example

```
#show ip vrf IPI
VRF IPI; (id=1); default RD 1:2
Interfaces:
  eth2
Export VPN route-target communities
  RT:100:1
Import VPN route-target communities
  RT:100:1
No import route-map
```

show ipv6 forwarding

Use this command to display IPv6 forwarding status.

Command Syntax

```
show ipv6 forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of the `show ipv6 forwarding` command displaying the IPv6 forwarding status.

```
#show ipv6 forwarding
ipv6 forwarding is on
#
```

show ipv6 interface

Use this command to display brief information about interfaces and the IPv6 address assigned to them. To display information about a specific interface, specify the interface name with the command.

Command Syntax

```
show ipv6 interface IFNAME brief
```

Parameters

`IFNAME`	Display the name of the interface.
`brief`	Brief summary of IPv6 status and configuration.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output from the `show ipv6 interface brief` command:

```
#show ipv6 interface brief
lo                        [up/up]
    ::1
gre0                      [administratively down/down]    unassigned
eth0                      [up/up]
    3ffe:abcd:104::1
    3ffe:abcd:103::1
    fe80::2e0:29ff:fe6f:cf0
eth1                      [up/up]
    fe80::260:97ff:fe20:f257
eth2                      [administratively down/down]    unassigned
eth3                      [administratively down/down]    unassigned
sit0                      [administratively down/down]    unassigned
tun24                     [administratively down/down]    unassigned
tunl0                     [administratively down/down]    unassigned
```


show ipv6 neighbors

Use this command to display all IPv6 neighbors.

Command Syntax

```
show ipv6 neighbors
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

```
#show ipv6 neighbors
 IPv6 Address                              MAC Address     Interface  Type
#
```

show ipv6 route

Use this command to display the IP routing table for a protocol or from a particular table, including database entries known by NSM. When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. The best routes are in the FIB and can be viewed by using `show ipv6 route` (see show ipv6 route on page 202 for more information).

Command Syntax

```
show ipv6 route vrf WORD (database|)
show ipv6 route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route (database|)
show ipv6 route (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route X:X::X:X
show ipv6 route X:X::X:X/M
show ipv6 route summary
```

Parameters

`X:X::X:X`	Display network in the IP routing table.
`X:X::X:X/M`	Display IP prefix <network>/<length>, e.g., 35.0.0.0/8.
`bgp`	Display Border Gateway Protocol (BGP) information.
`connected`	Display connected information.
`database`	Display IPv6 routing table database information.
`isis`	Display ISO IS-IS information.
`kernel`	Display kernel information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`static`	Display static routes.
`summary`	Display a summary of all routes
`vrf`	Display routes from a VPN Routing/Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Examples

The following is a sample output of the `show ipv6 route` command displaying the IPv6 routing table.

```
#show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info.
C> * ::1/128 is directly connected, lo
C> * 3ffe:1::/48 is directly connected, eth1
C> * 3ffe:2:2::/48 is directly connected, eth2
#
```


show ipv6 prefix-list

Use this command to display the prefix list entries for IPv6 interfaces.

Syntax Description

```
show ipv6 prefix-list
show ipv6 prefix-list WORD
show ipv6 prefix-list WORD seq <1-4294967295>
show ipv6 prefix-list WORD X:X::X:X/M
show ipv6 prefix-list WORD X:X::X:X/M longer
show ipv6 prefix-list WORD X:X::X:X/M first-match
show ipv6 prefix-list summary
show ipv6 prefix-list summary WORD
show ipv6 prefix-list detail
show ipv6 prefix-list detail WORD
```

Parameters

`WORD`	Name of a prefix list.
`X:X::X:X/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Lookup longer prefix.
`seq`	Sequence number of an entry.
`<1-4294967295>`	Actual sequence number.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Example

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

```
#show ipv6 prefix-list
ip prefix-list ipi1: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```

show hosts

Use this command to display the IP domain-name, lookup style and any name server.

Command Syntax

```
show hosts
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

```
#show hosts
```

show running-config interface

Use this command to show the running system status and configuration for a specified interface, or a specified interface for a specified protocol.

Command Syntax

```
show running-config interface IFNAME
show running-config interface IFNAME bridge
show running-config interface IFNAME dot1x
show running-config interface IFNAME elmi
show running-config interface IFNAME ip igmp
show running-config interface IFNAME ip multicast
show running-config interface IFNAME ip pim
show running-config interface IFNAME ipv6 ospf
show running-config interface IFNAME ipv6 rip
show running-config interface IFNAME ipv6 pim
show running-config interface IFNAME isis
show running-config interface IFNAME lacp
show running-config interface IFNAME ldp
show running-config interface IFNAME lmi
show running-config interface IFNAME mpls
show running-config interface IFNAME mstp
show running-config interface IFNAME ospf
show running-config interface IFNAME ptp
show running-config interface IFNAME rip
show running-config interface IFNAME rpvst+
show running-config interface IFNAME rstp
show running-config interface IFNAME rsvp
show running-config interface IFNAME stp
show running-config interface IFNAME trill
```

Parameters

`bridge`	Display bridge information.
`dot1x`	Display IEEE 802.1X port-based access control.
`elmi`	Display ELMI information.
`ip`	Display Internet Protocol version 4 (IPv4) (see also show running-config interface ip on page 207) information.
`ipv6`	Display Internet Protocol version 6 (IPv6) information (see also show running-config interface ipv6 on page 208) information.
`isis`	Display Intermediate System to Intermediate System (IS-IS) information.

`lacp`	Display Link Aggregation Control Protocol (LACP) information.
`ldp`	Display Label Distribution Protocol (LDP) information.
`lmi`	Display Local Management Interface (LMI) information.
`mpls`	Display Multiple Spanning Tree Protocol (MSTP) information.
`mstp`	Display Multiple Spanning Tree Protocol (MSTP) information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`ptp`	Display Precision Time Protocol (PTP) information.
`rip`	Display Routing Information Protocol (RIP) information.
`rpvst+`	Display Rapid Per VLAN Spanning Tree Protocol (RPVST) information.
`rstp`	Display Rapid Spanning Tree Protocol (RSTP) information.
`rsvp`	Display Resource Reservation Protocol (RSVP) information.
`stp`	Display Spanning Tree Protocol (STP) information.
`trill`	Display TRILL information.

Command Mode

Privileged Exec mode and Config Mode

Example

```
#show running-config interface eth1 bridge
!
interface eth1
 switchport
 bridge-group 1
 switchport mode access
 user-priority 3
 traffic-class-table user-priority 2 num-traffic-classes 3 value 3 traffic-
class-table user-priority 7 num-traffic-classes 1 value 2 traffic-class-table
user-priority 7 num-traffic-classes 2 value 0 traffic-class-table user-
priority 7 num-traffic-classes 3 value 0 traffic-class-table user-priority 7
num-traffic-classes 4 value 0 traffic-class-table user-priority 7 num-traffic-
classes 5 value 0 traffic-class-table user-priority 7 num-traffic-classes 6
```

show running-config interface ip

Use this command to show the running system status and configuration for a specified IP.

Command Syntax

```
show running-config interface IFNAME ip igmp
show running-config interface IFNAME ip multicast
show running-config interface IFNAME ip pim
```

Parameters

`igmp`	Display Internet Group Management Protocol (IGMP)
`multicast`	Display global IP multicast commands information.
`pim`	Display Protocol Independent Multicast (PIM) information.

Command Mode

Privileged Exec mode

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
 switchport
```

show running-config interface ipv6

Use this command to show the running system status and configuration for a specified IPv6 protocol.

Command Syntax

```
show running-config interface IFNAME ipv6 ospf
show running-config interface IFNAME ipv6 pim
show running-config interface IFNAME ipv6 rip
```

Parameters

`ospf`	Display Open Shortest Path First (OSPF) for IPv6 information.
`pim`	Display Protocol Independent Multicast (PIM) for IPv6 information.
`rip`	Display Routing Information Protocol (RIP) for IPv6 information.

Command Mode

Privileged Exec mode

Example

```
#show running-config interface eth1 ipv6 ospf
!
interface eth1
 switchport
```

show running-config ip

Use this command to show the running system of IP configurations.

Command Syntax

```
show running-config ip route
show running-config ip mroute
show running-config ip igmp
show running-config ip igmp snooping
show running-config ip pim
show running-config ip multicast
show running-config ip static bfd
```

Parameters

`igmp`	Display Internet Group Management Protocol (IGMP)
`snooping`	Layer 2 Snooping
`mroute`	Display static IP multicast route information.
`multicast`	Display global IP multicast information.
`pim`	Display Protocol Independent Multicast (PIM) information.
`route`	Display static IP route information.
`static bfd`	Display static BFD information.

Command Mode

Privileged Exec mode

Example

```
#show running-config interface eth1 ip multicast
!
ip multicast-routing
ip multicast route-limit 23
!

#show running-config ip pim
!
ip pim spt-threshold
ip pim accept-register list 1
!
>enable
#show running-config ip route
!
ip route 3.3.3.3/32 eth3
ip route 3.3.3.3/32 eth2
ip route 200.0.0.0/16 lo
!
```

show running-config ipv6

Use this command to show the running system status and configuration for IPv6.

Command Syntax

```
show running-config ipv6 access-list
show running-config ipv6 route
show running-config ipv6 mroute
show running-config ipv6 pim
show running-config ipv6 prefix-list
```

Parameters

`access-list`	Display access-list information.
`mroute`	Display static IP multicast route information.
`pim`	Display Independent Multicast (PIM) information.
`prefix-list`	Display prefix-list information.
`route`	Display static IP route information.

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config ipv6 access-list
!
ipv6 access-list abc permit any
!
#show running-config ipv6 prefix-list
!
ipv6 prefix-list sde seq 5 permit any
!
#show running-config ipv6 route
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 eth2
ipv6 route fe80::/64 eth2
!
```

shutdown

Use this command to shut down the selected interface.

Use the `no` form of this command to disable this function.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Command Mode

Interface mode

Examples

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

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

CHAPTER 6 Traffic Engineering Commands

This chapter provides a reference of the NSM Traffic Engineering (TE) command. Most commands are executed in TE link mode.

This chapter includes the following commands:

data-link

Use this command to associate data links with TE links. Only data-links can be associated to a TE link. Attempting to map multiple data links to the same TE link returns an error.

Use the `no` option with this command to remove an existing data link from a TE link.

Command Syntax

```
data-link IFNAME
no data-link IFNAME
```

Parameter

`IFNAME`	Indicate the interface name.

Command Mode

TE Link mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#data-link eth1

(config-te)#no data-link eth1
(config-te)#data-link eth2
```

description

Use this command to provide a TE Link-specific description.

Use the `no` option with this command to remove the description.

Command Syntax

```
description LINE
no description
```

Parameters

`LINE`	Text describing the specific interface.

Command Mode

TE Link mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#description This is for Testing
```

ip address

Use this command to set the IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address A.B.C.D/M
no ip address (A.B.C.D/M |)
```

Parameters

`A.B.C.D/M`	Specify the IP address and prefix length of an interface.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#ip address 10.10.10.50/24
```

label-switching

Use this command to enable label-switching on a TE link.

Use the no option with this command to disable label-switching on a TE link.

Command Syntax

```
label-switching
no label-switching
```

Parameters

None

Command Mode

TE Link mode

Example

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#label-switching
```

remote-link-id

Use this command to configure remote link id for each TE link.

Use the no option with this command to remove the remote link ID from a TE link.

Command Syntax

```
remote-link-id A.B.C.D
no remote-link-id (A.B.C.D|)
```

Parameters

A.B.C.D	Remote link ID in IPv4 address format.

Command Mode

TE Link mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#remote-link-id 172.1.2.3
```

reservable-bandwidth

Use this command to specify the maximum reservable bandwidth per interface. This value can be a larger or smaller value than `max-bandwidth`. When no max-reservable-bandwidth is specified, the default is equal to the `max-bandwidth`. Use the `no` parameter to remove the maximum reservable, and use the maximum bandwidth.

Use the `no` parameter with this command to disable the configuration.

Command Syntax

```
reservable-bandwidth BANDWIDTH
no reservable-bandwidth
```

Parameters

`BANDWIDTH`	Specify a bandwidth within the range of 1 to 999 kilobits (k), megabits (m) or gigabits (g). <1-10000000000 bits>.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#reservable-bandwidth 100m
```

show running-config te-link

Use this command to show the running system status of TE-link configurations.

Command Syntax

```
show running-config te-link
show running-config te-link TLNAME
```

Parameters

TLNAME	Display the TE link name

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config te-link new-te-123
!
```

show te-link

This command is used to display the properties for a particular TE link.

Command Syntax

```
show te-link (TLNAME|)
```

Parameter

TLNAME	Displays the name of a TE link.

Command Mode

Exec mode

Example

The following example is sample output for this command:

```
#show te-link te1
te-link te1
        description test
  Data-link: eth1
  Local link-id: 2.3.4.5
  Remote-link-id: 3
        IP address: 10.10.10.50/24
  Remote IP address: 10.10.10.51/24
  Index 2 mtu 1500
    <UP,POINT-TO-POINT,RUNNING >
  Control Adjacency: Rtr2
         Link ID: 22.2.2.2
    Administrative Group(s): None
  TE Metric 20
  Bandwidth 100m
  Maximum reservable bandwidth 70m
  DSTE Bandwidth Constraint Mode is MAM
    Bandwidth Constraint for Class Type default is 70m
  Available b/w for TE-CLASS 0 {a2, 5} is 0
    Maximum LSP b/w at Priority 0 is 0
  Maximum LSP b/w at Priority 1 is 0
        Maximum LSP b/w at Priority 2 is 70m
        Maximum LSP b/w at Priority 3 is 70m
        Maximum LSP b/w at Priority 4 is 70m
        Maximum LSP b/w at Priority 5 is 70m
        Maximum LSP b/w at Priority 6 is 70m
        Maximum LSP b/w at Priority 7 is 70m
  Minimum LSP Bandwidth is 10m
  Switching Capability: PSC1
  Encoding Type: Packet
  Protection: 1:1
  risk-group 2, 3
        mtu: 1500
#
```

shutdown

Use this command to shut down the selected TE link.

Use the `no` form of this command to disable this function.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Command Mode

TE Link mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#shutdown
```

te-link

Use this command to create a TE (traffic engineering) link and set its local-link-id.

Use the `no` option with this command to delete an existing TE link.

Command Syntax

```
te-link TLNAME
te-link TLNAME local-link-id A.B.C.D (numbered |)
no te-link TLNAME ((local-link-id A.B.C.D (numbered |))|)
```

Parameters

`TLNAME`	Name of the TE link.
`local-link-id`	Local link Identifier.
`A.B.C.D`	Local interface ID expressed in IPv4 address format.
`numbered`	The data link type is numbered.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1

#configure terminal
(config)#te-link te1 local-link-id 1.2.3.4

#configure terminal
(config)#te-link te1 local-link-id 1.2.3.4 numbered
```

CHAPTER 7 Control Channel Mode Commands

The commands in this chapter are issued in the NSM Control Channel mode. It includes the following commands:

control-channel

Use this command to create a new Control Channel. It is also used to identify a control-channel ID (`cc-id`), and designate the local and remote addresses used by the control channel.

Use the `no` option with this command to delete an existing Control Channel.

Command Syntax

```
control-channel CCNAME
control-channel CCNAME cc-id <1-4294967295> local-address A.B.C.D peer-address
  A.B.C.D
no control-channel CCNAME cc-id <1-4294967295> local-address A.B.C.D peer-address
  A.B.C.D
```

Parameters

`CCNAME`	Control channel name.
`cc-id`	Control channel parameters.
`<1-4294967295>`	Control channel ID value in integer format.
`local-address`	Control channel local address.
`A.B.C.D`	Control channel local address in IPv4 address format.
`peer-address`	Control channel local address.
`A.B.C.D`	Control channel peer address in IPv4 address format.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#control-channel cc1 cc-id 22 local-address 2.2.2.2 peer-address
4.4.4.4
(config-cc)#
```

description

Use this command to provide an Control Channel-specific description.

Use the `no` parameter to remove the description.

Command Syntax

```
description LINE
no description
```

Parameter

`LINE`	Characters describing this control channel.

Command Mode

Control Channel mode

Examples

```
(config)#control-channel new cc-id 123 local-address 123.4.5.67 peer-address
123.4.5.68
(config-cc)#description Connected to eth1

(config-cc)#no description
```

show control-channel

Use this command to display information about a control channel.

Command Syntax

```
show control-channel (CCNAME|)
```

Parameter

CCNAME	Specify name of the control channel.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of this command:

```
================================
Control-Channel : newer
  Gifindex : 20
  Local-address : 1.2.3.4
  Peer-address : 1.2.3.5
  Control-Channel ID : 12345
  Interface binding: N/A
  Belong to Control-Adjacency : N/A
  Status DOWN : admin Up   operational Down   NSM Down
  Last UP Time : 00:00:00
  Last Down Time : 20:17:55
================================
Control-Channel : new
  Description Control Channel specific description :
  Gifindex : 18
  Local-address : 1.2.3.4
  Peer-address : 1.2.3.4
  Control-Channel ID : 123
  Interface binding: N/A
  Belong to Control-Adjacency : N/A
  Status DOWN : admin Up   operational Down   NSM Down
  Last UP Time : 18:49:31
  Last Down Time : 18:49:27
================================
#
```

show running-config control-channel

Use this command to show the complete status and configuration of a control channel configuration.

Command Syntax

```
show running-config control-channel
show running-config control-channel CCNAME
```

Parameters

CC_NAME	Specify name of the control-channel.

Command Mode

Privileged Exec mode, Configure mode, Router mode

Example

```
(config)#show running-config control-channel
 no shutdown
 !
!
(config)#
```

shutdown

Use this command to shut down the selected control channel.

Use the `no` form of this command to disable this function.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Command Mode

Control Channel mode

Examples

The following example shows the use of the `shutdown` command.

```
(config)#control-channel new cc-id 123 local-address 123.4.5.67 peer-address
123.4.5.68
(config-cc)#shutdown

(config-cc)#no shutdown
```

CHAPTER 8 Control Adjacency Commands

The commands in this chapter are issued in the Control Adjacency mode. It includes the following commands:

control-adjacency

Use this command to create a new Control Adjacency with a neighbor router. The command also configures a peer address for the control adjacency, and provides the option to specify whether it is statically configured or should be managed using LMP.

Use the `no` option with this command to remove an existing control adjacency.

Command Syntax

```
control-adjacency CADJNAME peer-address A.B.C.D (static |using-lmp |)
no control-adjacency CADJNAME ((peer-address A.B.C.D (static |using-lmp|))|)
```

Parameters

`CADJNAME`	Control adjacency name in text format.
`A.B.C.D`	Control adjacency peer address in IPv4 address format.
`peer-address`	Control Adjacency Parameters.
`static`	Static configuration of control adjacency.
`using-lmp`	Control adjacency is managed using Link Management Protocol (LMP).

Command Mode

Configure mode

Example

```
#configure terminal
(config)#control-adjacency rtr2 peer-address 4.4.4.4 static
(config-ca)#
```

description

Use this command to provide a control adjacency-specific description.

Use the `no` parameter to remove the description.

Command Syntax

```
description LINE
no description
```

Parameter

`LINE`	Characters describing this control adjacency.

Command Mode

Control Adjacency mode

Examples

```
(config)#control-adjacency new peer-address 1.2.3.4 static
(config-ca)#description Connected to eth1

(config-ca)#no description
```

show control-adjacency

This command is used to display the properties for a particular Control Adjacency.

Command Syntax

```
show control-adjacency (CANAME|)
```

Parameter

CANAME	Name of the control adjacency

Command Mode

Exec Mode

Example

The following example is sample output for this command:

```
#show control-adjacency ca2
Control-channel Rtr2
description test
Control Channels: cc1, cc2
Primary Control Channel : cc1
TE Links: te1, te2
peer-address 3.3.3.3
index 2
<UP, RUNNING>
LMP is in USE
```

show running-config control-adjacency

Use this command to show the running system status and details for any control adjacency configuration.

Command Syntax

```
show running-config control-adjacency
show running-config control-adjacency CANAME
```

Parameter

CANAME	Indicate the control adjacency name.

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config control-adjacency
!
```

te-link

Use this command to configure a TE link name.

Use the `no` parameter to remove a TE link name.

Command Syntax

```
te-link TELNAME
```

```
no te-link TELNAME
```

Parameters

None

Command Mode

Control Adjacency mode

Examples

```
#configure terminal
(config)#control-adjacency new peer-address 1.2.3.4 static
(config-ca)#te-link new-link

(config)#control-adjacency new peer-address 1.2.3.4 static
(config-ca)#no te-link new-link
```

CHAPTER 9 Tunneling Commands

This chapter contains commands for IP tunneling.

interface tunnel

Use this command to create a new tunnel interface.

Use the `no` parameter to destroy the tunnel interface.

Command Syntax

```
interface tunnel <0-2147483647>
no interface tunnel <0-2147483647>
```

Parameter

`<0-2147483647>` Specify a tunnel interface number.

Default

Disabled

Command Mode

Configure mode

Example

```
#configure terminal
(config)#interface tunnel 100
(config-if)#
```

tunnel checksum

Use this command to enable a checksum feature for the tunnel. When configuring the tunnel checksum, make sure to:

- configure the tunnel checksum feature before configuring the tunnel source and destination.
- configure the tunnel checksum on both ends of the tunnel.

Use the `no` parameter to disable the feature.

Command Syntax

```
tunnel checksum
no tunnel checksum
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel checksum
(config-if)#tunnel source 192.168.1.1
(config-if)#tunnel destination 192.168.254.2
```

tunnel destination

Use this command to specify a tunnel destination address in an IPv4 portion.

Use the `no` parameter to undo the address.

Command Syntax

```
tunnel destination A.B.C.D
no tunnel destination
```

Parameter

`A.B.C.D`	Specify a tunnel destination IPv4 address.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 200
(config-if)#tunnel mode ipip
(config-if)#tunnel source 10.10.0.1
(config-if)#tunnel destination 10.11.0.1
```

tunnel dmac

Use this command to set a destination MAC address for tunneled packets. This command supports IP-in-IP tunneling on Broadcom.

Use the `no` option with this command to remove the destination MAC address.

Command Syntax

```
tunnel dmac/mac MAC
no tunnel dmac
```

Parameter

`MAC`	Destination address in MAC format.

Default

If a specific MAC address is not set with this command, all tunneled packets are sent with a destination address of 0.

Command Mode

Interface mode

Examples

```
broadcom(config)#interface tunnel 7
broadcom(config-if)#tunnel mac 1213.2322.123
```

tunnel mode

Use this command to configure an IPv4 tunnel mode. This command specifies a tunnel encapsulation mode for either GRE and IPIP mode The GRE tunnel mode is used for IPv4-to-IPv4 tunneling.

Use the `no` parameter to remove the configuration from a mode.

Command Syntax

```
tunnel mode (ipip|gre)
no tunnel mode
```

Parameters

`ipip`	IPIP tunnel mode.
`gre`	Generic Routing Encapsulation (GRE) tunnel mode.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface tunnel 2
(config-if)#tunnel source 192.168.1.1
(config-if)#tunnel destination 192.168.2.1
(config-if)#tunnel mode gre
```

tunnel mode ipv6ip

Use this command to configure an IPv6 tunnel mode. This command specifies a tunnel encapsulation mode for either GRE and IPIP mode The GRE tunnel mode is used for IPv6-to-IPv6 tunneling.

Use the `no` parameter to remove the configuration from a mode.

Command Syntax

```
tunnel mode ipv6ip (6to4|isatap|)
no tunnel mode
```

Parameters

`6to4`	IPv6 automatic tunnelling using 6to4.
`isatap`	IPv6 automatic tunnelling using ISATAP.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel source 10.10.1.1
(config-if)#tunnel destination 10.10.2.1
(config-if)#tunnel mode ipv6ip 6to4
```

tunnel path-mtu-discovery

Use this command to enable path Maximum Transmission Unit (MTU) discovery in the underlying tunnel interface.

Use the `no` parameter to disable this feature.

Command Syntax

```
tunnel path-mtu-discovery
no tunnel path-mtu-discovery
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel source 192.168.0.1
(config-if)#tunnel destination 10.0.0.1
(config-if)#tunnel path-mtu-discovery
```

tunnel source

Use this command to specify a tunnel source address in a IPv4 portion.

Use the `no` parameter to undo the tunnel source address.

Command Syntax

```
tunnel source A.B.C.D
no tunnel source
```

Parameter

`A.B.C.D`	IPv4 tunnel source address.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel destination 10.10.1.1
(config-if)#tunnel source 10.11.2.1
```

tunnel tos

Use this command to specify a value of Type of Service (TOS) in the tunnel IPv4 encapsulation header.

Use the `no` parameter to make `0` the default value.

Command Syntax

```
tunnel tos <0-255>
no tunnel tos
```

Parameter

`<0-255>`	Specify a type of service integer.

Default

The default TOS value is 0.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel destination 192.168.10.2
(config-if)#tunnel source 192.168.11.1
(config-if)#tunnel tos 10
```

tunnel ttl

Use this command to specify a value of Time to Live (TTL) in the tunnel IPv4 encapsulation header. Enable the `path-mtu-discovery` before setting the TTL value. However, the first time you set the TTL value, and the `path-mtu-discovery` is not set, the system automatically enables the `path-mtu-discovery`.

Use the `no` parameter to inheriting the underlying physical interface value by default.

Command Syntax

```
tunnel ttl <1-255>
no tunnel ttl <1-255>
```

Parameter

`<1-255>`	Specify a Time to Live integer.

Default

By default, physical interface value is inherited.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel destination 192.168.128.1
(config-if)#tunnel source 192.168.0.1
(config-if)#tunnel ttl 255
```

CHAPTER 10 Internet Protocol Security Commands

This chapter provides an alphabetized reference for each of the Internet Protocol Security CLI commands. It includes the following commands:

address

Use this command to set the peer address in the policy.

Use the `no` form of this command to unset the peer address.

Command Syntax

```
address [A.B.C.D]
no address [A.B.C.D]
```

Parameters

`A.B.C.D`	Specify the peer IP address.

Command Mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#address 10.12.11.2
(config-isakmp)#exit
```

authentication

Use this command in ISAKMP policy configuration mode to specify the authentication method within an IKE policy. IKE policies define a set of parameters to be used during IKE negotiation.

The commands in this section are all entered in the ISAKMP policy configuration (config-isakmp) mode. To invoke this mode, use the `crypto isakmp policy` command in global configuration mode.

Use the `no` form of this command to reset the authentication method to the default value.

Command Syntax

```
authentication (pre-share)
no authentication
```

Parameters

`pre-share`	Preshared keys

Command Mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#authentication pre-share
(config-isakmp)#exit
```

clear crypto isakmp

Use this command to reset active IKE connections in Exec configuration mode.

Command Syntax

```
clear crypto isakmp
```

Parameters

None

Command Mode

Exec mode

Example

```
ZebOS#clear crypto isakmp
```

clear crypto sa map

Use this command to restart specific IPsec connection with given map name.

If you make changes in policy, that affect security associations, these changes will not apply to existing security associations, until we config this command.

Command Syntax

```
clear crypto sa map [MAP_NAME]
```

Parameter

MAP_NAME	Specify the name of the Crypto map to be reset.

Command Mode

Exec mode

Example

```
#clear crypto sa map t1
```

clear crypto sa

Use this command to reset IPSec security associations either for all peers or for the specified peer.

If you make configuration changes that affect security associations, these changes will not apply to existing security associations.

Command Syntax

```
clear crypto sa
clear crypto sa ipv4 peer A.B.C.D
clear crypto sa ipv6 peer X:X::X:X
```

Parameter

`A.B.C.D`	Specify the IPv4 address of the peer.
`X:X::X:X`	Specify the IPv6 address of the peer.

Command Mode

Exec mode

Example

```
#clear crypto sa
#clear crypto sa ipv4 peer 10.10.12.2
#clear crypto sa ipv6 peer 1001::2
```

crypto ipsec security-association lifetime

Use this command in global configuration mode to change global lifetime values used when negotiating IPSec security associations.

Use the `no` form of the command to reset a lifetime to the default value.

Command Syntax

```
crypto ipsec security-association lifetime seconds [LIFETIME]
no crypto ipsec security-association lifetime seconds
```

Parameters

`seconds`	Specify the number of seconds the security association will live before expiring.
`LIFETIME`	Specify the lifetime value of security association range <120-2592000> in seconds.

Defaults

None

Command Mode

Configure mode

Usage

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its global lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations. If the local lifetime is also defined for a crypto map then the local value overrides the global value.

Use the `clear crypto sa` command, to clear all or part of the security association database.

The lifetime values are ignored for manually established security associations.

Example

```
ZebOS(config)#crypto ipsec security-association lifetime seconds 15000
ZebOS(config)#no crypto ipsec security-association lifetime seconds
```

crypto ipsec transform-set

Use this command in global configuration mode to define a transform set—an acceptable combination of security protocols and algorithms.

Use the `no` form of the command to delete a transform set.

Command Syntax

```
crypto ipsec transform-set [NAME] esp-auth (none|esp-md5|esp-sha1) esp-enc (esp-
  null|esp-3des|esp-aes|esp-aes192|esp-aes256|esp-blf|esp-blf192|esp-blf256|esp-
  cast)
no crypto ipsec transform-set [NAME]
```

Parameters

`NAME`	Name of the transform set.
`esp-auth`	Set ESP Authentication Algorithm.
`none`	No Authentication Algorithm.
`esp-md5`	MD5 Authentication Algorithm
`esp-sha1`	Alternative SHA1 Authentication Algorithm.
`esp-enc`	Set ESP Encryption Algorithm
`esp-null`	Null encryption algorithm.
`esp-3des`	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES).
`esp-aes`	Alternative AES algorithm.
`esp-aes192`	Alternative AES192 algorithm.
`esp-aes256`	Alternative AES256 algorithm.
`esp-blf`	Alternative Blowfish algorithm.
`esp-blf192`	Alternative Blowfish192 algorithm.
`esp-blf256`	Alternative Blowfish256 algorithm.
`esp-cast`	Alternative Cast algorithm (ikev1 not supported) .

Command Mode

Configure mode

Usage

A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPSec protected traffic. Before a transform set can be included in a crypto map entry it must be defined using this command.

Example

```
ZebOS(config)#crypto ipsec transform-set t1 esp-auth esp-md5 esp-enc esp-aes
```

crypto isakmp enable

Use this command to globally enable IKE (Internet Key Exchange).

Use the `no` form of this command to disable IKE at the peer.

Command Syntax

```
crypto isakmp enable
no crypto isakmp enable
```

Parameters

None

Default

IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

Command Mode

ISAKMP policy configuration mode (config-isakmp)

Usage

This command should be configured at the end, after other parameters are configured. If we want to change some other parameter after configuring `crypto isakmp enable`, then first we have use the unconfigure this command.

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#crypto isakmp enable
```

crypto isakmp policy

Use this command to define an IKE policy in global configuration mode. IKE policies define a set of parameters to be used during the IKE negotiation. These parameters are used to create the IKE security association [SA]. This command invokes the ISAKMP policy configuration (config-isakmp) mode.

Use the `no` form of this command to delete an IKE policy.

Command Syntax

```
crypto isakmp policy PRIORITY
no crypto isakmp policy PRIORITY
```

Parameter

`PRIORITY`	Uniquely identifies the IKE policy and assigns a priority to the policy. Ranges from <1-10000>

Command mode

Configure mode

Example

```
ZebOS(config)#crypto isakmp policy 1
```

crypto map (Configure Mode)

Use this command in global configuration mode to create a crypto map entry and enter into the crypto map configuration mode.

Once a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, once a map entry has been created as ipsec-isakmp, you cannot change it to ipsec-manual; you must delete and re-enter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the `crypto map [map-name] (interface IPSec)` command.

Use the `no` form of this command to delete a crypto map entry or set.

Command Syntax

```
crypto map [MAP-NAME] (SEQ-NUM) (ipsec-manual|ipsec-isakmp)
no crypto map [MAP-NAME] (SEQ-NUM|)
```

Parameters

`MAP-NAME`	The name you assign to the crypto map set.
`SEQ-NUM`	The number you assign to the crypto map entry
`ipsec-manual`	Indicate that IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
`ipsec-isakmp`	Indicate that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.

Command mode

Configure mode

Example

```
ZebOS(config)#crypto map MAP1 1 ipsec-manual
ZebOS(config)#crypto map MAP1 1 ipsec-isakmp
```

crypto map (Interface Mode)

Use this command in interface configuration mode to apply a previously defined crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPSec services. Only one crypto map set can be assigned to an interface.

Use the `no` form of the command to remove the crypto map set from the interface.

Command Syntax

```
crypto map [MAP-NAME]
no crypto map [MAP-NAME]
```

Parameter

`MAP-NAME`	The name you assign to the crypto map set.

Command mode

Interface mode

Example

```
ZebOS(config)#interface eth1
ZebOS(config-if)#crypto map MAP1
```

crypto map local-address

Use this command to specify an interface to be used by the crypto map for IPSec traffic.

Use the `no` form of the command to remove this command from the configuration.

Command Syntax

```
crypto map [MAP-NAME] local-address [INTERFACE-ID]
no crypto map [MAP-NAME] local-address
```

Parameters

`MAP-NAME`	The name that identifies the crypto map set.
`INTERFACE-ID`	Specify an interface that should be used by the router to send traffic to peers.

Command mode

Configure mode

Example

```
ZebOS(config)#crypto map MAP1 local-address p7p1
```

encryption

Use this command to specify the encryption algorithm within an IKE policy in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.

This command is entered in the ISAKMP policy configuration (config-isakmp) mode. To invoke this mode, use the `crypto isakmp policy` command in global configuration mode.

Use the `no` form of this command to reset the encryption algorithm to the default value.

Command Syntax

```
encryption (aes|3des)
no encryption
```

Parameters

`aes`	Specify 56-bit DES-CBC as the encryption algorithm.
`3des`	Specify 168-bit DES (3DES) as the encryption algorithm.

Default

The default value is aes.

Command mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#encryption 3des
(config-isakmp)#exit
```

group

Use this command to specify the Diffie-Hellman group identifier within an IKE policy in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.

This command is entered in the ISAKMP policy configuration (config-isakmp) mode. To invoke this mode, use the `crypto isakmp policy` command in global configuration mode.

Use the no form of this command to reset the Diffie-Hellman group identifier to the default value.

Command Syntax

```
group (1|2|14)
no group
```

Parameters

`1`	Indicates group number 1- 768 bits long.
`2`	Indicates group number 2- 1024 bits long.
`14`	Indicates group number 14- 2048 bits long.

Defaults

2048-bits Diffie-Hellman (group 14)

Command mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#group 1
(config-isakmp)#exit
```

hash

Use this command to specify the hash algorithm within an IKE policy in ISAKMP policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.

This command is entered in the ISAKMP policy configuration (config-isakmp) mode. To invoke this mode, use the `crypto isakmp policy` command in global configuration mode.

Use the no form of this command to reset the hash algorithm to the default SHA-1 hash algorithm.

Command Syntax

```
hash (md5|sha1)
no hash
```

Parameters

`md5`	Specify MD5 (HMAC variant) as the hash algorithm.
`sha1`	Specify SHA-1 (HMAC variant) as the hash algorithm.

Default

Default is the SHA-1 hash algorithm.

Command mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#hash md5
(config-isakmp)#exit
```

ipv6-address

Use this command to set the IPv6 peer address.

Use the no form of this command to unset the IPv6 peer address.

Command Syntax

```
ipv6-address X:X::X:X
no ipv6-address X:X::X:X
```

Parameters

X:X::X:X	Specify the IPv6 peer address.

Command mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#ipv6-address 1001::2
(config-isakmp)#exit
```

ike-version

Use this command to set the IKE version.

Use the no form of this command to set the IKE version to default

Command Syntax

```
ike-version (1|2|both)
no ike-version
```

Parameters

1	Specify Internet Key Exchange Version (IKE-version) 1
2	Specify Internet Key Exchange Version (IKE-version) 2.
both	Specify Internet Key Exchange Version (IKE-version) 1/2 (default).

Command mode

ISAKMP policy configuration mode (config-isakmp)

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#ike-version 1
(config-isakmp)#exit
```

lifetime

Use the lifetime (IKE policy) command in ISAKMP policy configuration mode to specify the lifetime of an IKE security association (SA). To invoke this mode, use the `crypto isakmp policy` command in global configuration mode.

Use the `no` form of this command to reset the SA lifetime to the default value.

Command Syntax

```
lifetime LIFETIME
no lifetime
```

Parameter

`LIFETIME`	Specify how many seconds each SA should exist before expiring. Ranges between <60-86400>.

Defaults

10, 800 seconds

Command mode

ISAKMP policy configuration mode (config-isakmp)

Usage

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New IPSec SAs are negotiated before current IPSec SAs expire.

So, to save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#lifetime 15000
```

match address

Use this command in crypto map configuration mode to specify an extended IPv4 access list for a crypto map entry and also to inject security policy in SPDB in kernel.

Use the `no` form of this command to remove the extended access list from a crypto map entry.

Command Syntax

```
match address ACCESSLIST-ID
no match address ACCESSLIST-ID
```

Parameters

`ACCESSLIST-ID`	Identify the extended access list by its number.

Command mode

Crypto map configuration mode

Usage

Use this command to assign an extended access list to a crypto map entry. You also need to define this access list using the access-list or ip access-list extended commands. The extended access list specified with this command will be used by IPSec to determine which traffic should be protected by crypto and which traffic does not need crypto protection. Traffic that is permitted by the access list will be protected. Note that the crypto access list is not used to determine whether to permit or deny traffic through the interface.

The crypto access list specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists specified by the interface's crypto map entries to determine if it should be protected by crypto and if so (if traffic matches a permit entry) which crypto policy applies. After passing the regular access lists at the interface, outbound traffic is evaluated against the crypto access lists specified by the entries of the interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (In the case of IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#match address 101
(config-crypto)#exit
```

match ipv6-address

Use this command in crypto map configuration mode to specify an extended IPv6 access list for a crypto map entry and also to inject security policy in SPDB in kernel.

Use the `no` form of this command to remove the extended access list from a crypto map entry.

Command Syntax

```
match ipv6-address ACCESSLIST-NAME
no match ipv6-address ACCESSLIST-NAME
```

Parameters

`ACCESSLIST-NAME`	Identify the extended access list by its name.

Command mode

Crypto map configuration mode

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#match ipv6-address asdf
```

psk key

Use this command to set the PSK key, which is used in pre-share authentication mode by IKE while establishing IPsec connection with the peer.

Use the `no` form of this command to unset the PSK key.

Command Syntax

```
psk key KEY
no psk key KEY
```

Parameters

`KEY`	Specify the KEY value.Maximum length is 128

Command mode

ISAKMP policy configuration mode

Example

```
#configure terminal
(config)#crypto isakmp policy 1
(config-isakmp)#psk key v+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL
```

set peer

Use this command in crypto map configuration mode, to specify an IPSec peer in a crypto map entry.

Use the `no` form of this command to remove an IPSec peer from a crypto map entry.

Command Syntax

```
set peer [A.B.C.D]
no set peer [A.B.C.D]
```

Parameters

`A.B.C.D`	IPv4 address.

Command mode

Crypto map configuration mode

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#set peer 1.1.1.1
```

set ipv6 peer

Use this command in crypto map configuration mode, to specify an IPv6 peer in a crypto map entry.

Use the `no` form of this command to remove an IPv6 peer from a crypto map entry.

Command Syntax

```
set ipv6 peer [X:X::X:X]
no set ipv6 peer [X:X::X:X]
```

Parameters

`X:X::X:X`	Specify IPv6 address.

Command mode

Crypto map configuration mode

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#set ipv6 peer 1001::1


(config-crypto)#no set ipv6 peer 1001::1
```

set security-association lifetime

Use this command in crypto map configuration mode to override the global lifetime value for a particular crypto map entry.

Use the `no` form of this command to reset a crypto map entry's lifetime value to the global value.

Command Syntax

```
set security-association lifetime seconds [LIFETIME]
no set security-association lifetime seconds
```

Parameters

`seconds`	Specify the number of seconds a security association will live before expiring
`LIFETIME`	Specify the lifetime value of security association in the range <120-2592000>.

Command mode

Crypto map configuration mode

Usage

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its crypto map lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#set security-association lifetime seconds 15000

(config-crypto)#no set security-association lifetime seconds
```

set session-key

Use this command in crypto map configuration mode to manually specify the IPSec session keys within a crypto map entry. This command is only available for ipsec-manual crypto map entries.

Use the `no` form of this command to remove IPSec session keys from a crypto map entry.

Command Syntax

```
set session-key (inbound|outbound) esp SPI cipher (HEX-KEY-DATA) authenticator
  (HEX_KEY_DATA)
no set session-key (inbound|outbound) esp
```

Parameters

`inbound`	Sets the inbound IPSec session key.
`outbound`	Sets the outbound IPSec session key.
`esp`	Sets the IPSec session key for the ESP protocol.
`SPI`	Specify the security parameter index (SPI), a number that is used to uniquely identify a security association.
`HEX-KEY-DATA`	Specify the encryption key; enter in hexadecimal format.
`HEX-KEY-DATA`	Specify the authentication key; enter in hexadecimal format.

Command mode

Crypto map configuration mode

Usage

Use this command to define IPSec keys for security associations via ipsec-manual crypto map entries. (In the case of ipsec-isakmp crypto map entries, the security associations with their corresponding keys are automatically established via the IKE negotiation.)

Security associations established via this command do not expire (unlike security associations established via IKE). The inbound session key of one peer should be equal to the outbound session key of other peer and the outbound session key of one peer should be equal to the inbound session key of other peer. The cipher length depends upon the esp protocol defined in the transform set which is attached to the crypto-map.

The following list the crypto encryption key lengths:

Encryption type	Cipher length in bits
`null`	<8-512>
`3des`	192
`cast`	<40-128>
`blf128`	<32-128>

Encryption type	Cipher length in bits
blf192	<136-192>
blf256	<200-448>
aes128	128
aes192	192
aes256	256

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#set session-key inbound esp 1 cipher ABCE authenticator EFGH
```

set transform-set

Use this command in crypto map configuration mode to specify which transform set can be used with the crypto map entry.

Use the `no` form of this command to remove transform set from a crypto map entry.

Command Syntax

```
set transform-set [NAME]
no set transform-set [NAME]
```

Parameter

`NAME`	The name that identifies the crypto map set

Command mode

Crypto map configuration mode

Usage

If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

Example

```
#configure terminal
(config)#crypto map new 5 ipsec-isakmp
(config-crypto)#set transform-set new
```

show crypto ipsec transform-set

Use this command to view all the configured transform sets or specific transform set.

To modify the lines displayed, use the | (output modifier token). To save the output to a file, use the > output redirection token.

Command Syntax

```
show crypto ipsec transform-set (NAME|)
```

Parameter

NAME	Display the transform set name.

Command mode

Exec mode

Example

```
ZebOS#show crypto ipsec transform-set t1
Transform set t1
  Mode is Tunnel
  Algorithm esp-aes esp-md5
```

show crypto isakmp policy

Use this command to view the parameters for each IKE policy in Exec mode.

To modify the lines displayed, use the | (output modifier token). To save the output to a file, use the > output redirection token.

Command Syntax

```
show crypto isakmp policy
```

Parameters

None

Command mode

Exec mode

Example

```
ZebOS#show crypto isakmp policy
Protection suite priority 1
  encryption algorithm:   3DES - Data Encryption Standard
  hash algorithm:   Message Digest 5
  authentication method:   preshared Key
  Diffie-Hellman Group: #14 (modp2048)
  lifetime: 15000
 psk key: v+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL
 peer address: 11.11.11.2
```

show crypto map

Use this command to view the crypto map configuration.

To modify the lines displayed, use the | (output modifier token). To save the output to a file, use the > output redirection token.

Command Syntax

```
show crypto-map [interface (IFNAME)]
```

Parameter

IFNAME	Display interface name.

Command mode

Exec mode

Example

```
ZebOS#sh crypto-map interface p7p1
Interface p7p1
Crypto-map MAP1
Crypto-spi 0
Crypto-access-list-name
Crypto-Transform set t1
Crypto-map peer: 11.11.11.2
```

show ipsec status

Use this command to view the IP security status.

Command Syntax

```
show ipsec status
```

Parameter

None

Command mode

Exec mode

Example

```
ZebOS#show ipsec status
Security Associations (1 up, 0 connecting):
       map1-1[1]: ESTABLISHED 5 minutes ago,
11.11.11.1[11.11.11.1]...11.11.11.2[11.11.11.2]
       map1-1{6}: INSTALLED, TUNNEL, ESP SPIs: c492556c_i ccf5790f_o
       map1-1{6}: 11.11.11.1/32 === 11.11.11.2/32
       map1-1{6}: INSTALLED, TUNNEL, ESP SPIs: cb43a379_i cedc90fc_o
       map1-1{6}: 11.11.11.1/32 === 11.11.11.2/32
```

CHAPTER 11 Remote Monitoring Commands

This chapter provides an alphabetized reference for each Remote Monitoring (RMON) CLI command. It includes the following commands:

rmon alarm

Use this command to configure alarm parameters, such as, alarm type, thresholds, and corresponding events on crossing the threshold for a particular variable.

Use the `no` form of this command to remove the alarm configuration.

Command Syntax

```
rmon alarm <1-65535> (WORD) interval <1-4294967295> (delta | absolute) rising-
  threshold event <0-65535> falling-threshold event <0-65535> alarmstartup <1-3>
  (owner WORD|)
no rmon alarm <1-65535>
```

Parameters

`<1-65535>`	Alarm entry index value.
`WORD`	Variable Object Identifier (OID) name to be monitored.
`interval`	Polling interval in seconds <1-4294967295>.
`delta`	Alarm sample type of delta.
`absolute`	Alarm sample type of absolute.
`rising-threshold`	
	Rising threshold value of the alarm entry.
`event`	Event corresponding to the alarm crossing the rising threshold value of the alarm entry <0-65535>.
`falling-threshold`	
	Falling threshold value of the alarm entry.
`event`	Event corresponding to the alarm crossing the falling threshold value of the alarm entry <0-65535>.
`owner`	Owner name to identify entry.
`alarmstartup`	Specify alarm startup type.
`<1-3>`	Specify alarm startup value.

Default

No default alarm is created.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#rmon alarm 229 etherStatsEntry.1.5 interval 50 delta rising-threshold
400 event 70 falling-threshold 600 event 1 owner new
```

rmon clear

Use this command to clear RMON counters.

Command Syntax

```
rmon clear counters
```

Parameters

`counters`	Clears RMON counters.

Command Mode

Interface mode

Example

```
(config-if)#rmon clear counters
```

rmon collection history

Use this command to configure a history statistics control group. History statistics parameters can be requested buckets, interval and owner name on a particular interface. The number of history statistics buckets, and the interval to collect them, can be specified. The system based on the available memory configures the granted buckets. The granted buckets are same as the requested buckets.

Use the `no` form of this command to remove the history control configuration.

Command Syntax

```
rmon collection history <1-65535> (buckets <1-65535>|)(interval <1-3600>|) (owner
  WORD|)
no rmon collection history <1-65535>
```

Parameters

`<1-65535>`	Alarm entry index value.
`interval`	Polling interval in seconds <1-4294967295>.
`buckets`	Number of requested buckets <1-65535>.
`owner`	Owner name to identify entry.

Default

No default alarm is created.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth1
(config-if)#rmon collection history 200 buckets 500 interval 600 owner herbert
```

rmon collection stats

Use this command to configure an Ethernet statistics parameter, such as, index and owner name, on a particular interface.

Use the `no` form of this command to remove the collection statistics configuration.

Command Syntax

```
rmon collection stats <1-65535> (owner WORD|)
no rmon collection stats <1-65535>
```

Parameters

`<1-65535>`	Specify buckets history index <1-65535>. Default is 50.
`owner`	Owner name to identify entry.

Default

Ethernet statistics probe is not running.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth1
(config-if)#rmon collection stats 200 owner herbert
```

rmon debug

Use this command to specify the set of debug options for RMON.

Use the `no` parameter with this command to disable the debugging option.

Command Syntax

```
rmon debug
no rmon debug
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

```
#rmon debug
```

rmon event

Use this command to configure event parameters, such as, event type, description, and the community string corresponding to the trap if the event type is trap. The configured trap community does not take effect as the trap sending is handled by the SNMP daemon.

Use the `no` form of this command to remove the event configuration.

Command Syntax

```
rmon event <1-65535> (log |)(trap WORD |) (description WORD|) (owner WORD|)
no rmon event <1-65535>
```

Parameters

`<1-65535>`	Event entry index value.
`log`	Log event type
`trap`	Trap event type
`description`	Event entry description
`owner`	Owner name to identify entry.
`WORD`	Community string corresponding to the trap

Default

No default event is created.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#rmon event 299 log description cond3 owner alfred
```

show rmon alarm

Use this command to display the alarms and threshold configured for the RMON probe.

Command Syntax

```
show rmon alarm
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon alarm
```

show rmon event

Use this command to display the events configured for the RMON probe.

Command Syntax

```
show rmon event
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon event
```

show rmon history

Use this command to display the history Ethernet statistics collected on a particular interface.

Command Syntax

```
show rmon history
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon history
```

show rmon statistics

Use this command to display the Ethernet statistics collected on a particular interface.

Command Syntax

```
show rmon statistics
```

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon statistics
```

snmp restart rmon

Use this command to restart SNMP in Remote Monitoring (RMON).

Command Syntax

```
snmp restart rmon
```

Parameters

None

Command Mode

Configure mode

Examples

```
(config)#snmp restart rmon
```

CHAPTER 12 Unicast Reverse Path Forwarding Check

This chapter provides an alphabetized reference for each of the Unicast Reverse Path Forwarding (uRPF) commands. It includes the following commands:

- ip verify unicast source reachable-via
- ipv6 verify unicast source reachable-via

ip verify unicast source reachable-via

Use this command to enable Unicast Reverse Path Forwarding (uRPF) checking on the interface for IPv4. The interface should be a Layer 3 type.

Use the no form of this command to disable uRPF checking.

Command Syntax

```
ip verify unicast source reachable-via {any [allow-default] | rx}
no ip verify unicast source reachable-via
```

Parameters

`any`	Loose mode: source is reachable via any interface; the source IP address for a packet must appear in the routing table
`allow-default`	Allow default route to match when checking source address; otherwise, a default route is not considered in loose mode
`rx`	Strict mode: source is reachable via the interface on which the packet was received

Command Mode

Interface mode

Examples

```
(config-if)#ip verify unicast source reachable-via rx
(config-if)#ip verify unicast source reachable-via any

(config-if)#no ip verify unicast source reachable-via
```

ipv6 verify unicast source reachable-via

Use this command to enable Unicast Reverse Path Forwarding (uRPF) checking on the interface for IPv6. The interface should be a Layer 3 type.

Use the no form of this command to disable uRPF checking.

Command Syntax

```
ipv6 verify unicast source reachable-via {any [allow-default] | rx}
no ipv6 verify unicast source reachable-via
```

Parameters

`any`	Loose mode: source is reachable via any interface; the source IP address for a packet must appear in the routing table
`allow-default`	Allow default route to match when checking source address; otherwise, a default route is not considered in loose mode
`rx`	Strict mode: source is reachable via the interface on which the packet was received

Command Mode

Interface mode

Examples

```
(config-if)#ipv6 verify unicast source reachable-via rx
(config-if)#ipv6 verify unicast source reachable-via any

(config-if)#no ipv6 verify unicast source reachable-via
```

Index

D

E

G

H

I

L

M

N

P

R

S

T

V

W