FortiSwitchOS CLI Reference

VERSION 3.6.4

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

August 20, 2019

FortiSwitchOS-3.6.4 CLI Reference

TABLE OF CONTENTS

Change Log

Date	Change Description
January 12, 2018	Initial version for release 3.6.4
August 20, 2019	Updated the “config system snmp user” section.

Introduction

This manual describes the command line interface (CLI) commands for FortiSwitchOS.

FortiSwitch models

This guide is applicable to all FortiSwitch models that are supported by FortiSwitchOS.

See the Release Notes for information about the software features supported on each of the models.

How this guide is organized

The chapters in this document describe the commands available for each of the top-level CLI commands:

- config—commands that allow you to configure various components of the FortiSwitch.
- diagnose—commands that help with troubleshooting.
- execute—commands that perform immediate operations.
- get—commands that provide information about FortiSwitch operation.

Typographical conventions

This document uses the following typographical conventions:

Convention	Example

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system setting`
	`comments  : (No default)`
	`opmode  : nat`

Emphasis	HTTP connections are **not** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>

Convention	Example
Hyperlink	Visit the Fortinet Technical Support web site: https://support.fortinet.com
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Publication	For details, see the FortiOS Handbook.

CLI command syntax conventions

This guide uses the following conventions to describe the syntax to use when entering commands in the Command Line Interface (CLI).

Convention	Description
Angle brackets `< >`	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`.
Data types include:	
`<xxx_name>`	A name referring to another part of the configuration, such as `policy_A`.
`<xxx_index>`	An index number referring to another part of the configuration, such as `0` for the first static route.
`<xxx_pattern>`	A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`.
`<xxx_fqdn>`	A fully qualified domain name (FQDN), such as `mail.example.com`.
`<xxx_email>`	An email address, such as `admin@mail.example.com`.
`<xxx_ipv4>`	An IPv4 address, such as `192.168.1.99`.
`<xxx_v4mask>`	A dotted decimal IPv4 netmask, such as `255.255.255.0`.
`<xxx_ipv4mask>`	A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`.

Convention	Description
`<xxx_ipv4/mask>`	A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`.
`<xxx_ipv6>`	A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`.
`<xxx_ipv6mask>`	An IPv6 netmask, such as `/96`.
`<xxx_ipv6/mask>`	An IPv6 address and netmask separated by a space.
`<xxx_int>`	An integer number that is **not** another data type, such as `15` for the number of minutes.
`<xxx_url>`	A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet./com/`.
Square brackets `[ ]`	A non-required word or series of words. For example: [verbose {1 | 2 | 3}] indicates that you can either omit or type both the `verbose` word and its accompanying option, such as: `verbose 3`
Curly braces `{ }`	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
Options delimited by vertical bars `|`	Mutually exclusive options. For example: {enable | disable} indicates that you must enter either `enable` or `disable` but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: `ping https ssh` **NOTE:** To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type: `ping https snmp ssh` If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Entering configuration data

The switch configuration is stored as a series of configuration settings in the FortiSwitchOS configuration database. To change the configuration, you can use the CLI to add, delete, or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

Entering text strings (names)

Text strings are used to name entities in the configuration, such as an administrative user name. You can enter any character in a text string with the following exceptions (to prevent cross-site scripting vulnerabilities):

- " (double quote)
- & (ampersand)
- ' (single quote)
- < (less than)
- < (greater than)

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the CLI allows for a given name field. From the CLI, you can also use the `tree` command to view the number of characters that are allowed. For example, firewall address names can contain up to 64 characters. From the CLI, you can do the following to confirm that the firewall address name field allows 64 characters:

```
config firewall address
   tree
         -- [address] --*name (64)
         |- subnet
         |- type
         |- start-ip
         |- end-ip
         |- fqdn (256)
         |- cache-ttl (0,86400)
         |- wildcard
         |- comment (64 xss)
         |- associated-interface (16)
         +- color (0,32)
```

NOTE: The tree command output also shows the number of characters allowed for other firewall address name settings. For example, the fully qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example, the IP address 10.10.10.1) or, as in the case of MAC or IPv6 addresses, separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (such as MAC addresses) require hexadecimal numbers.

CLI help includes information about allowed numeric value ranges.The CLI prevents you from entering invalid numbers.

config

Use the `config` commands to configure various components of the FortiSwitch:

config log

Use the `config log` commands to set the logging type, the logging severity level, and the logging location for the system:

config log custom-field

Use the following command to customize the log fields with a name and/or value. The custom name and/or value will appear in the log message.

Syntax

```
config log custom-field
   edit <id>
      set name <name>
      set value <int>
   end
```

Variable	Description	Default
<id >	Enter the identification string for the custom log .	No default
name <name>	Enter a name to identify the log. You can use letters, numbers, (‘_‘), but no special characters such as the number symbol (#). The name cannot exceed 16 characters.	No default

Variable	Description	Default
value <int>	Enter an integer value to associate with the log.	No default

Example

This example shows how to configure a customized field for a log:

```
config log custom-field
   edit 1
      set name "Vlan"
      set value 3
end
```

config log eventfilter

Use this command to configure event logging.

Syntax

```
config log eventfilter
   set event {enable | disable}
   set router {enable | disable}
   set system {enable | disable}
   set user {enable | disable}
end
```

Variable	Description	Default
event {enable | disable}	Log event messages. Must be enabled to make the following fields available.	enable
router {enable | disable}	Log router activity messages.	enable
system {enable | disable}	Log system activity messages.	enable
user {enable | disable}	Log user activity messages.	enable

Example

This example shows how to configure event logging:

```
config log eventfilter
   set event enable
   set router enable
   set system enable
   set user enable
end
```

config log gui

Use this command to select the device from which logs are displayed in the Web-based manager.

Syntax

```
config log gui
   set log-device memory
end
```

Variable	Description	Default
log-device memory	Select the device from which logs are displayed in the Web-based manager. Currently, only logging to memory is available.	memory

config log memory filter

Use this command to configure the filter for the memory buffer.

Syntax

```
config log memory filter
   set severity {alert | critical | debug | emergency | error |
       information | notification | warning}
end
```

Variable	Description	Default
severity {alert | critical | debug | emergency | error | information | notification | warning}	Select the logging severity level. The system logs all messages at and above the logging severity level you select. For example, if you select `error`, the system logs `error`, `critical`, `alert` and `emergency` level messages. • `emergency` — The system is unusable. • `alert` — Immediate action is required. • `critical` — Functionality is affected. • `error` — An erroneous condition exists and functionality is probably affected. • `warning`— Functionality might be affected. • `notification` — Information about normal events. • `information` — General information about system operations. • `debug` — Information used for diagnosing or debugging the system.	information

Example

This example shows how to configure the memory log filter:

```
config log memory filter
   set severity alert
end
```

config log memory global-setting

Use this command to configure log threshold warnings, as well as the maximum buffer lines, for the FortiSwitch system memory.

The FortiSwitch system memory has a limited capacity and displays only the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the system begins to overwrite the oldest log messages. All log entries are deleted when the system restarts.

Syntax

```
config log memory global-setting
   set full-final-warning-threshold <int>
   set full-first-warning-threshold <int>
   set full-second-warning-threshold <int>
   set hourly-upload {disable | enable}
   set max-size <int>
end
```

Variable	Description	Default
full-final-warning-threshold <int>	Enter to configure the final warning before reaching the threshold. You can enter a number between 3 and 100.	95
full-first-warning-threshold <int>	Enter to configure the first warning before reaching the threshold. You can enter a number between 1 and 98.	75
full-second-warning-threshold <int>	Enter to configure the second warning before reaching the threshold. You can enter a number between 2 and 99.	90
hourly-upload {disable | enable}	Enter `enable` to have log uploads occur hourly.	disable
max-size <int>	Enter the maximum size of the memory buffer log, in bytes.	98304

Example

This example shows how to configure log threshold warnings and the maximum buffer lines:

```
config log memory global-setting
   set full-final-warning-threshold 45
   set full-first-warning-threshold 25
   set full-second-warning-threshold 45
   set hourly-upload enable
   set max-size 12288
end
```

config log memory setting

Use this command to configure log settings for logging to the system memory.

The system memory has a limited capacity and only displays the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the system begins to overwrite the oldest messages. All log entries are deleted when the system restarts.

Syntax

```
config log memory setting
   set status {disable | enable}
   set diskfull overwrite
end
```

Variable	Description	Default
status {disable | enable}	Enter `enable` to enable logging to system memory.	disable
diskfull overwrite	Overwrite the oldest log when the log device is full.	No default

Example

This example shows how to configure log settings:

```
config log memory setting
   set status enable
   set diskfull overwrite
end
```

config log {syslogd | syslogd2 | syslogd3} filter

Use this command to configure log filter options. Log filters define the types of log messages sent to each log location.

Syntax

```
config log {syslogd | syslogd2 | syslogd3} filter
   set severity {alert | critical | debug | emergency | error |
       information | notification | warning}
end
```

Variable	Description	Default
severity {alert | critical | debug | emergency | error | information | notification | warning}	Select the logging severity level. The system logs all messages at and above the logging severity level you select. For example, if you select `error`, the system logs `error`, `critical`, `alert` and `emergency` level messages. • `emergency` — The system is unusable. • `alert` — Immediate action is required. • `critical` — Functionality is affected. • `error` — An erroneous condition exists and functionality is probably affected. • `warning`— Functionality might be affected. • `notification` — Information about normal events. • `information` — General information about system operations. • `debug` — Information used for diagnosing or debugging the system.	information
status {enable | disable}	Enable or disable remote syslog logging.	disable

Example

This example shows how to configure log filter options:

```
config log syslogd filter
   set severity information
end
```

config log {syslogd | syslogd2 | syslogd3} setting

Use this command to configure log settings for logging to the system memory.

The system memory has a limited capacity and only displays the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the system begins to overwrite the oldest messages. All log entries are deleted when the system restarts.

Syntax

```
config log {syslogd | syslogd2 | syslogd3} setting
   set status {disable | enable}
   set server <server_name>
   set reliable disable
   set port <port_number>
   set csv {enable | disable}
   set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel |
       local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail
       | news | ntp | syslog | user | uucp}
   set source-ip <IPv4_address>
end
```

Variable	Description	Default
status {disable | enable}	Enter `enable` to enable logging to system memory.	disable
server <server_name>	This field is available with `status` is set to `enable`. Enter the address of the remote syslog server.	No default
reliable disable	This field is available with `status` is set to `enable`. Disable the reliable delivery for syslog.	disable
port <port_number>	This field is available with `status` is set to `enable`. Set the port number that the server listens to.	514
csv {enable | disable}	This field is available with `status` is set to `enable`. Enable or disable comma-separated values.	disable
set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}	This field is available with `status` is set to `enable`. Select the facility for remote syslog: • `alert`—Use the log alert. • `audit`—Use the log audit. • `auth`—Use the security/authorization messages. • `authpriv`—Use the private security/authorization messages. • `clock`—Use the clock daemon. • `cron`—Use the clock daemon. • `daemon`—Use the system daemon. • `ftp`—Use the FTP daemon. • `kernel`—Use kernel messages. • `local0`—Reserved for local use. • `local1`—Reserved for local use. • `local2`—Reserved for local use. • `local3`—Reserved for local use. • `local4`—Reserved for local use. • `local5`— Reserved for local use. • `local6`— Reserved for local use. • `local7`—Reserved for local use. • `lpr`—Use the line printer subsystem. • `mail`—Use the mail system. • `news`—Use the network news subsystem. • `ntp`—Use the NTP system. • `syslog`—Use memssages generated internally by the syslog daemon. • `user`—Use random user-level messages. • `uucp`—Use the network news subsystem.	local7
source-ip <IPv4_address>	This field is available with `status` is set to `enable`. Enter the source IPv4 address of the syslog.	0.0.0.0

Example

This example shows how to configure log settings:

```
config log syslogd setting
   set status enable
   set server "1.2.3.4"
   set port 5
end
```

config router

Use the `config router` commands to configure options related to routing protocols and packet forwarding:

config router access-list

Use this command to configure an access list for RIP routing. An access list is a list of IP addresses and the action to take for each one. Access lists provide basic route and network filtering.

Syntax

```
config router access-list
   edit <list_str>
      set comments <comment_str>
      config rule
         edit <rule_int>
            set action {deny | permit}
            set prefix {<xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> | any}
            set wildcard <ip>
            set exact-match {enable | disable}
      end
   end
```

Variable	Description	Default
<list_str>	Enter the name of the access list.	No default
comments <comment_str>	Enter a descriptive comment.	No default
<rule_int>	The rule identifier.	No default

Variable	Description	Default
action {deny | permit}	Set whether the rule allows or denies the IP address.	permit
prefix {<xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> | any}	Set the prefix to define regular filter criteria, such as any or subnets. Do not use for Cisco-style access lists.	any
wildcard <ip>	Define Cisco-style wildcard filter criteria.	No default
exact-match {enable | disable}	Set whether the rulee looks for an exact match with the value in the prefix field.	disable

Example

This example shows how to configure an access list:

```
config router access-list
   edit mylist
      set comments "access list for RIP 1"
      config rule
         edit 1
            set action permit
            set prefix xxx.xx.xx.xx xxx.xxx.xxx.x
   end
end
```

config router key-chain

Use this command to configure a keychain for RIP version 2 routing. A keychain is a list of one or more authentication keys including its lifetime, which is how long each key is valid. Use keys with overlapping lifetimes to prevent the failure of routing updates.

NOTE: You must create a keychain first before you can use the MD5 authentication mode with RIP version 2.

Syntax

```
config router key-chain
   edit <keychain_name>
      config key
         edit <keychain_int>
            set key-string <key_str>
            set accept-lifetime <START> <END>
            set send-lifetime <START> <END>
         end
      end
   end
```

Variable	Description	Default
<keychain_name>	Enter a name for your keychain.	No default
<keychain_int>	Enter the keychain identifier.	No default

Variable	Description	Default
key-string <key_str>	Enter a password string for the key.	No default
accept-lifetime <START> <END>	Enter the lifetime of a received authentication key. START and END use the format of HH:MM:SS DAY MONTH YEAR where: • HH:MM:SS is the time of day then the lifetime starts in hours, minutes, and seconds. • DAY is the day of the month to start. The range is 1-31. • MONTH is the month of the year to start. The range is 1-12. • YEAR is the year to start. The range is 1993-2035. END can also be set to `infinite` or <duration>, which is the number of seconds that the key is valid. the range of <duration> is 1-2147483646.	No default
send-lifetime <START> <END>	Enter the lifetime of a sent authentication key. START and END use the format of HH:MM:SS DAY MONTH YEAR where: • HH:MM:SS is the time of day then the lifetime starts in hours, minutes, and seconds. • DAY is the day of the month to start. The range is 1-31. • MONTH is the month of the year to start. The range is 1-12. • YEAR is the year to start. The range is 1993-2035. END can also be set to `infinite` or <duration>, which is the number of seconds that the key is valid. the range of <duration> is 1-2147483646.	No default

Example

This example shows how to add a key to a new keychain:

```
config router key-chain
   edit keychain1
      config key
         edit 1
            set key-string 1234567890
            set accept-lifetime 01:02:03 1 8 2017 infinite
            set send-lifetime 01:02:03 1 8 2017 infinite
         end
      end
```

config router ospf

Use this command to configure OSPF routing.

NOTE: You must have an advanced features license to use OSPF routing.

Open shortest path first (OSPF) is a link-state interior routing protocol that is widely used in large enterprise organizations. OSPF provides routing within a single autonomous system (AS). This differs from BGP, which provides routing between autonomous systems.

An OSPF AS can contain only one area, or it may consist of a group of areas connected to a backbone area. A router connected to more than one area is an area border router (ABR). Routing information is contained in a link state database. Routing information is communicated between routers using link state advertisements (LSAs).

You can enable bidirectional forwarding detection (BFD) with OSPF. BFD is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and, if a timer runs out on a connection, that router is declared to be down. BFD then communicates this information to OSPF, and the routing information is updated.

Syntax

```
config router ospf
   set router-id <router_ipv4>
   set abr-type {cisco | ibm | shortcut | standard}
   set distance-external <external_int>
   set distance-inter-area <inter_int>
   set distance-intra-area <intra_int>
   set default-information-originate {always | disable | enable}
   set default-information-metric <metric_int>
   set default-information-metric-type {1 | 2}
   set default-information-route-map <map_str>
   set distance <distance_int>
   set rfc1583-compatible {disable | enable}
   set spf-timers <delay_int> <hold_int>
   set bfd {disable | enable}
   set log-neighbour-changes {disable | enable}
   set passive-interface {<name_str> | internal | mgmt}
   config area
      edit <area_ipv4>
         set authentication {md5 | none | text}
         set shortcut {default | disable | enable}
         set type {nssa | regular | stub}
         set default-cost <cost_int>
         set stub-type {no-summary | summary}
         set nssa-translator-role {always | candidate | never}
         config filter-list
            edit <filter_int>
               set direction {in | out}
               set list <list_str>
            end
         end
         config range
            edit <range_int>
               set advertise {enable | disable}
               set prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
               set substitute <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
               set substitute {enable | disable}
            end
         end
         config virtual-link
            edit <virtual_int>
               set authentication {md5 | none | text}
               set dead-interval <dead_int>
```

```
            set hello-interval <hello_int>
            set peer <peer_ipv4>
            set retransmit-interval <retransmit_int>
            set transmit-delay <transmit_int>
         end
      end
   end
   config ospf-interface
      edit <interface_str>
         set authentication {md5 | none | text}
         set bfd {disable | enable | global}
         set cost <cost_int>
         set dead-interval <dead_int>
         set hello-interval <hello_int>
         set interface {<string> | internal | mgmt}
         set mtu <mtu_int>
         set mtu-ignore {disable | enable}
         set priority <pritority_int>
         set retransmit-interval <retransmit_int>
         set transmit-delay <transmit_int>
      end
   end
   config network
      edit <network_int>
         set area <area_ipv4>
         set prefix <xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx>
      end
   end
   config distribute-list
      edit <distribute_int>
         set access-list <access_str>
         set protocol {connected | rip | static}
      end
   end
   config redistribute {<name_str> | connected | rip | static}
      set status {disable | enable}
      set metric <metric_int>
      set routemap <routemap_str>
      set metric-type {1 | 2}
   end
end
```

Variable	Description	Default
router-id <router_ipv4>	Enter the IPv4 address of the OSPF router.	No default
abr-type {cisco | ibm | shortcut | standard}	Enter the area border router (ABR) type. Set `abr-type` to `cisco` or `ibm` to allow routes through nonbackbone area when links to the backbone are down. For more information about this option, see RFC 3509, Alternative Implementations of OSPF Area Border Routers.	cisco

Variable	Description	Default
distance-external <external_int>	Set the OSPF route administrative external distance. The value range is from 0 to 255.	0
distance-inter-area <inter_int>	Set the OSPF route administrative inter-area distance. The value range is from 0 to 255.	0
distance-intra-area <intra_int>	Set the OSPF route administrative intra-area distance. The value range is from 0 to 255.	0
default-information-originate {always | disable | enable}	Enable or disable the generation of the default route into all external routing capable areas using the metric specified by the `default-information-metric` value and the metric type specified by the `default-information-metric-type` value. Set the value to `always` for the default to always be advertised, even when the routing table contains no default.	disable
default-information-metric <metric_int>	Set the metric value for the default route. The value range is from 1 to 16777214.	10
default-information-metric-type {1 | 2}	Set the metric type for the default route.	2
default-information-route-map <map_str>	Enter the name of the route map.	No default
distance <distance_int>	Enter the distance of the route. The value range is from 1 to 255.	**110**
rfc1583-compatible {disable | enable}	Enable or disable RFC1583 compatibility.	disable
spf-timers <delay_int> <hold_int>	Set the number of seconds before the shortest path first (SPF) is calculated and the number of seconds between consecutive SPF calculations. The range for each value is from 0 to 600.	5 10
bfd {disable | enable}	Enable or disable bidirectional forwarding detection (BFD).	disable
log-neighbour-changes {disable | enable}	Enable or disable the logging of changes to the OSPF neighbor	enable
passive-interface {<name_str> | internal | mgmt}	Select which interface to set to passive mode.	No default
config area		
<area_ipv4>	Enter the IP address for the area.	No default

Variable	Description	Default
authentication {md5 | none | text}	Set the authentication type for OSPF packets.	none
shortcut {default | disable | enable}	Enable or disable whether shortcuts are allowed in the area.	default
type {nssa | regular | stub}	Set the area type.	regular
default-cost <cost_int>	If the area type is stub or not-so-stubby area (NSSA), set the cost of default-summary link state advertisements (LSAs) announced to stubby areas. The value range is 0-2147483647.	1
stub-type {no-summary | summary}	If the area type is stub or NSSA, set whether inter-area summaries can be used.	summary
nssa-translator-role {always | candidate | never}	If the area type is NSSA, set the type of NSSA translator role.	candidate
config filter-list		
<filter_int>	Enter the filter list identifier.	No default
direction {in | out}	Set the direction to or from the area for the prefix list and access list.	out
list <list_str>	Enter the access-list name or prefix-list name for the area.	No default
config range		
<range_int>	Enter the range list identifier.	No default
advertise {enable | disable}	Enable or disable the advertise status. If this option is set to `disable`, the intra area paths from this range are not advertised in other areas.	enable
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the summary prefix.	0.0.0.0 0.0.0.0
substitute <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the substitute prefix.	0.0.0.0 0.0.0.0
substitute {enable | disable}	Enable or disable whether the substitute prefix is used instead of the prefix.	disable
config virtual-list		
<virtual_int>	Enter the virtual-link identifier.	No default

Variable	Description	Default
authentication {md5 | none | text}	Set the authentication type.	none
dead-interval <dead_int>	Enter the dead interval.	40
hello-interval <hello_int>	Enter the hello interval.	10
peer <peer_ipv4>	Enter the IP address of the virtual link neighbor.	0.0.0.0
retransmit-interval <retransmit_int>	Enter the retransmit interval.	5
transmit-delay <transmit_int>	Enter the transmit delay.	1
config ospf-interface		
<interface_str>	Enter the OSPF interface name.	No default
authentication {md5 | none | text}	Set the authentication type for OSPF packets.	none
bfd {disable | enable | global}	Enable or disable BFD on this interface. Set this option to `global` to use the global configuration.	global
cost <cost_int>	Enter the link cost on this interface. The value range is 0-65535. Set this option to 0 for auto-cost.	10
dead-interval <dead_int>	Enter the dead interval.	40
hello-interval <hello_int>	Enter the hello interval.	10
interface {<string> | internal | mgmt}	Set the interface.	No default
mtu <mtu_int>	Enter the maximum transmission unit (MTU) size in bytes for the database description packets. The value range is 576-65535.	1500
mtu-ignore {disable | enable}	Set whether to use the MTU size.	disable
priority <priority_int>	Set the router priority for this interface. the router with the highest priority is more eligible to become the designated router. Setting the option to 0 makes the router ineligible to become the designated router. The value range is 0-255.	1
retransmit-interval <retransmit_int>	Enter the retransmit interval.	5

Variable	Description	Default
transmit-delay <transmit_int>	Enter the transmit delay.	1
config network		
<network_int>	Enter the network identifier.	No default
<area_ipv4>	Enter the IP address for the area.	No default
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the prefix.	0.0.0.0 0.0.0.0
config distribute-list		
<distribute_int>	Enter the distribute list identifier.	No default
access-list <access_str>	Enter the access list name.	No default
protocol {connected | rip | static}	Set the protocol type.	connected
config redistribute {<name_str> | connected | rip | static}		
redistribute {<name_str> | connected | rip | static}	Set the type of network to redistribute.	No default
status {disable | enable}	Enable or disable the redistribution.	disable
metric <metric_int>	Enter the metric for redistributed routes.	10
routemap <routemap_str>	Enter the route map name to filter the redistributed routes.	No default
metric-type {1 | 2}	Set the metric type of redistributed routes.	2

Example

This example shows how to set the router identifier, create an area, create the network (set the network prefix and associate with an area), configure the OSPF interface, and redistribute the routes:

```
config router ospf

   set router-id 10.11.101.1

   config area
      edit 0.0.0.0
      next
   end

   config network
      edit 1
         set area 0.0.0.0
         set prefix 10.11.101.0 255.255.255.0
```

```
      next
   end

   config ospf-interface
      edit "1"
         set cost 100
         set interface "vlan10"
         set priority 100
      next
   end

   config redistribute connected
      set status enable
   end

end
```

config router prefix-list

Use this command to configure prefix-based filtering for RIP routing.

NOTE: You must have an advanced features license to use RIP routing.

Syntax

```
config router prefix-list
   edit <list_int>
      set comments <comment_str>
      config rule
         edit <rule_int)
            set action {deny | permit}
            set {prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> | any}
            set ge <ge_int>
            set le <le_int>
         end
      end
   end
```

Variable	Description	Default
<list_int>	Enter the prefix list identifier.	No default
comments <comment_str>	Enter a descriptive comment.	No default
rule_int	Enter the rule identifier.	No default
action {deny | permit}	Set the action to `deny` or `permit`.	permit
{prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx> | any}	Set the prefix to define regular filter criteria, such as any or subnets.	0.0.0.0 0.0.0.0

Variable	Description	Default
ge <ge_int>	Enter the minimum prefix length to be matched. The value range is between 0 and 32. The prefix list is used if the prefix length is greater than or equal to this value.	No default
le <le_int>	Enter the maximum prefix length to be matched. The value range is between 0 and 32. The prefix list is used if the prefix length is less than or equal to this value.	No default

config router rip

Use these commands to configure RIP routing.

NOTE: You must have an advanced features license to use RIP routing.

The Routing Information Protocol (RIP) is a distance-vector routing protocol that works best in small networks that have no more than 15 hops. Each router maintains a routing table by sending out its routing updates and by asking neighbors for their routes. RIP is relatively simple to configure on FortiSwitch units but slow to respond to network outages. RIP is better than static routing but less scalable than open shortest path first (OSPF).

FortiSwitch supports RIP version 1 and RIP version 2:

- RIP version 1 uses classful addressing and broadcasting to send out updates to router neighbors. It does not support different sized subnets or classless inter-domain routing (CIDR) addressing.
- RIP version 2 supports classless routing and subnets of various sizes. Router authentication supports MD5 and authentication keys. Version 2 uses multicasting to reduce network traffic.

RIP uses three timers:

- The update timer determines the interval between routing updates. The default setting is 30 seconds.
- The timeout timer is the maximum time that a route is considered reachable while no updates are received for the route. The default setting is 180 seconds. The timeout timer setting should be at least three times longer than the update timer setting.
- The garbage timer is the is the how long that the FortiSwitch advertises a route as being unreachable before deleting the route from the routing table. The default setting is 120 seconds.

You can enable bidirectional forwarding detection (BFD) with RIP. BFD is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and, if a timer runs out on a connection, that router is declared to be down. BFD then communicates this information to RIP, and the routing information is updated.

Syntax

```
config router rip
   set bfd {disable | enable}
   set default-information-originate {disable | enable}
   set default-metric <defaultmetric_int>
   set garbage-timer <garbage_int>
   set passive-interface {<name_str> | internal | mgmt}
   set timeout-timer <timeout_int>
   set update-timer <update_int>
   set version {1 | 2}
   config distance
```

```
      edit <distanceid_int>
         set access-list <access_string>
         set distance <distance_int>
         set prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
      end
   config distribute-list
      edit <distribute_int>
         set direction {in | out}
         set interface <interface_str>
         set listname <listname_str>
         set status {disable | enable}
      end
   config interface
      edit <interface_str>
         set auth-keychain <keychain_str>
         set auth-mode {md5 | none |text}
         set auth-string <password_str>
         set receive-version {1 | 2 | both |global}
         set send-version {1 | 2 | both |global}
         set split-horizon-status {disable | enable}
         set split-horizon {poisoned | regular}
      end
   config neighbor
      edit <neighbor_int>
         set <neighbor_ipv4>
      end
   config network
      edit <network_int>
         set prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
      end
   config offset-list
      edit <offsetlist_int>
         set access-list <accesslist_str>
         set direction {in | out}
         set interface {in | out}
         set offset <offset_int>
         set status {disable | enable}
      end
   config redistribute {<name> | connected | ospf | static}
      set status {disable | enable}
      set metric <metric_int> (between 0 and 16)
      set routemap <routemap_str>
   end
end
```

Variable	Description	Default
bfd {disable | enable}	Enable or disable BFD.	disable
default-information-originate {disable | enable}	Enable or disable whether a default route is advertised.	disable

Variable	Description	Default
default-metric <defaultmetric_int>	Enter the default metric for redistributed routes. This setting does not affect connected routes. Use the `config redistribute connected` or `config offset-list` command to set the metric value for connected routes.	1
garbage-timer <garbage_int>	Enter the number of seconds before a route is removed from the routing table.	120
passive-interface {<name_str> | internal | mgmt}	Specify which interface to set to passive mode. In passive mode, multicast and unicast RIP packets are sent only to RIP neighbors.	No default
timeout-timer <timeout_int>	Enter the number of seconds before a route is no longer valid. The route is not removed from the routing table until the neighboring RIP routers are notified that the route has been dropped.	180
update-timer <update_int>	Enter the number of seconds between when the complete routing table is sent to neighboring RIP routers.	30
version {1 | 2}	Set the RIP version for receiving and sending RIP packets.	2
config distance		
<distanceid_int>	Enter the distance identifier.	No default
access-list <access_string>	Enter the access list for the route destination. The default RIP distance is used only when the route's source IP address matches the specified prefix *and* the specified access list.	No default
distance <distance_int>	Enter the default RIP distance. The value range is from 1 to 255. The default RIP distance is used only when the route's source IP address matches the specified prefix *and* the specified access list.	120
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the prefix.	0.0.0.0 0.0.0.0
config distribute-list		
<distribute_int>	Enter the distribute list identifier.	No default
direction {in | out}	Set the list direction.	out
interface <interface_str>	Enter the RIP interface name for the distribute list.	No default

Variable	Description	Default
listname <listname_str>	Enter the access or prefix list name.	No default
status {disable | enable}	Enable or disable whether the distribute list is used.	disable
config interface		
<interface_str>	Enter the interface name.	No default
auth-keychain <keychain_str>	Enter the name of the keychain to use for this interface.	No default
auth-mode {md5 | none | text}	Set the authentication mode used for packets. RIP version 1 does not use authentication. If `auth-mode` is set to `md5` or `text` for RIP version 1, routing updates are ignored. **NOTE:** You must create a keychain first before you can use the MD5 authentication mode with RIP version 2.	none
auth-string <password_str>	If the `auth-mode` is set to `text`, enter a password that is less than 16 characters long.	No default
receive-version {1 | 2 | both | global}	Set which version of RIP packets are accepted on this interface. Setting this option to `both` accepts RIP version 1 and 2. Setting this option to `global` uses the global RIP version. This setting overrides the global RIP version setting.	global
send-version {1 | 2 | both | global}	Set which version of RIP packets are sent for this interface. Setting this option to `both` sends RIP version 1 and 2. Setting this option to `global` uses the global RIP version. This setting overrides the global RIP version setting.	global
split-horizon-status {disable | enable}	Enable or disable split horizon.	enable
split-horizon {poisoned | regular}	Set the split-horizon type.	regular
config neighbor		
<neighbor_int>	Enter a RIP neighbor identifier.	No default
<neighbor_ipv4>	Enter an IP address for a RIP neighbor. Use this command if a RIP neighbor does not accept multicast packets.	0.0.0.0
config network		

Variable	Description	Default
<network_int>	Enter a network identifier.	No default
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the prefix.	0.0.0.0 0.0.0.0
config offset-list		
<offsetlist_int>	Enter the offset list identifier.	No default
<accesslist_str>	Enter the name of the access list.	No default
direction {in | out}	Set the list direction.	out
interface {in | out}	Set whether to filter incoming or outgoing packets.	No default
offset <offset_int>	Enter the offset for incoming and outgoing metrics to routes learned using RIP. The value range is between 1 and 16.	0
status {disable | enable}	Enable or disable whether the offset list is used.	disable
config redistribute {<name> | connected | ospf | static}		
redistribute {<name> | connected | ospf | static}	Redistribute routes so that they are included in RIP routing. By default, connected, ospf, and static are disabled.	<name>
status {disable | enable}	Enable or disable whether the routes are redistributed.	disable
metric <metric_int>	Enter the metric of the redistributed routes. The value range is between 0 and 16.	0
routemap <routemap_str>	Enter the route map name to filter the redistributed routes.	No default

Example

This example shows how to configure the RIP router and add authentication:

```
config router rip
   config network
      edit 1
         set prefix 170.38.65.0/24
      next
      edit 2
         set prefix 128.8.0.0/16
      next
   end
   config interface
      edit "vlan35"
         set auth-mode text
         set auth-string simplepw1
```

```
      next
   end
end
```

config router route-map

Use this command to configure a route map for OSPF or RIP routing.

NOTE: You must have an advanced features license to use OSPF or RIP routing.

Syntax

```
config router route-map
   edit <routemap_str>
      set comments <comments_str>
      set protocol {ospf | rip}
      config rule
         edit <rule_int>
            set action {deny | permit}
            set match-interface {<interface_str> | internal | mgmt}
            set match-ip-address <address_str>
            set match-ip-nexthop <nexthop_str>
            set match-metric <metric_int>
            set match-tag <tag_int>
            set set-ip-nexthop <class_ipv4>
            set set-metric <setmetric_int>
            set set-metric-type {1 | 2}
            set set-tag <settag_int>
         end
      end
   end
```

The dst and gateway fields are required when blackhole is disabled. When blackhole is enabled, the dst field is required. All other fields are optional.

Variable	Description	Default
<routemap_str>	Enter the name of the route map.	No default
comments <comments_str>	Enter a descriptive comment.	No default
protocol {ospf | rip}	Set the protocol to OSPF or RIP.	No default
<rule_int>	Enter the rule identifier.	No default
action {deny | permit}	Set whether the rule permits or denies the item.	permit
match-interface {<interface_str> | internal | mgmt}	Set which interface will be matched.	No default

Variable	Description	Default
match-ip-address <address_str>	Match the IP address permitted by the access list or prefix list.	No default
match-ip-nexthop <nexthop_str>	Match the next-hop IP address passed by the access list or prefix list.	No default
match-metric <metric_int>	RIP only. Enter the metric to be matched for redistributed routes. The value range is 0-2147483647.	0
match-tag <tag_int>	RIP only. Enter the tag to be matched. The value range is 0-2147483647.	0
set-ip-nexthop <class_ipv4>	RIP only. Enter the IP address of the next hop.	0.0.0.0
set-metric <setmetric_int>	Enter the route metric value. The value range is 0-2147483647.	0
set-metric-type {1 | 2}	OSPF only. Set the metric type to external-type1 or external-type2.	external-type1
set-tag <settag_int>	RIP only. Enter the route tag value. The value range is 0-2147483647.	0

Example

This example shows how to configure the RIP router and add authentication:

```
config router route-map
   edit myroutemap
      set comments "route map for RIP routing"
      set protocol rip
      config rule
         edit 1
            set action permit
            set match-interface internal
            set match-metric 12
            set match-tag 36
            set set-ip-nexthop 128.8.0.0
            set auth-mode text
            set set-metric 48
            set set-tag 72
      end
   end
```

config router setting

Use this command to set which routing table to use.

NOTE: You must have an advanced features license to use OSPF or RIP routing.

Syntax

```
config router setting
   config filter-list
      edit <routemap_int>
         set protocol {any | connected | ospf | rip | static}
         set route-map <routemap_str>
      end
   end
```

Variable	Description	Default
<routemap_int>	Enter a route map identifier.	No default
protocol {any | connected | ospf | rip | static}	Set which protocol this route map applies to.	connected
route-map <routemap_str>	Enter the route map name.	No default

Example

This example shows how to configure the RIP router and add authentication:

```
config router setting
   config filter-list
      edit 2
         set protocol ospf
         set route-map myroutemap
      end
   end
```

config router static

Use this command to add, edit, or delete static routes for IPv4 traffic.

You add static routes to manually control traffic exiting the FortiSwitch. You configure routes by specifying destination IP addresses and network masks and adding gateways for these destination addresses. Gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.

You can adjust the administrative distance of a route to indicate preference when more than one route to the same destination is available. The lower the administrative distance, the greater the preferability of the route. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the system compares the administrative distances of those entries, selects the entries having the lowest distances, and installs them as routes in the FortiSwitch forwarding table. Any ties are resolved by comparing the routes' priority, with lowest priority being preferred. As a result, the forwarding table only contains routes having the lowest distances to every possible destination.

After the system selects static routes for the forwarding table based on their administrative distances, the sequence numbers of those routes determines routing priority. When two routes to the same destination exist in the forwarding table, the system selects the route having the lowest sequence number.

Syntax

```
config router static
   edit <sequence_number>
```

```
    set bfd {enable | disable | global}
    set blackhole {enable | disable}
    set comment <comment_str>
    set device <interface_name>
    set distance <distance>
    set dst <destination-address_ipv4mask>
    set dynamic-gateway {enable | disable}
    set gateway <gateway-address_ipv4>
    set priority <integer>
    set weight <integer>
end
```

The `dst` and `gateway` fields are required when `blackhole` is disabled. When `blackhole` is enabled, the `dst` field is required. All other fields are optional.

Variable	Description	Default
<sequence_number>	Enter a sequence number for the static route. The sequence number may influence routing priority in the forwarding table.	No default
bfd {enable | disable | global}	Enable or disable Bidirectional Forwarding on this interface. If you set the value to global, the BFD value for this interface is the same as the global BFD value.	
blackhole {enable | disable}	Enable or disable dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route.	disable
comment <comment_str>	Optionally enter a descriptive comment.	No default
device <interface_name>	This field is available when `blackhole` is set to `disable`. Enter the name of the interface through which to route traffic. Use '?' to see a list of interfaces.	No default
distance <distance>	Enter the administrative distance for the route. The distance value may influence route preference in the routing table. The range is an integer from 1-255.	10
dst <destination-address_ ipv4mask>	Enter the destination IPv4 address and network mask for this route. You can enter `0.0.0.0/0` to create a new static default route.	0.0.0.0/0
dynamic-gateway {enable | disable}	When enabled, dynamic-gateway hides the gateway variable for a dynamic interface, such as a DHCP or PPPoE interface. When the interface connects or disconnects, the corresponding routing entries are updated to reflect the change.	disable

Variable	Description	Default
gateway <gateway-address_ipv4>	This field is available when `blackhole` is set to `disable`. Enter the IPv4 address of the next-hop router to which traffic is forwarded.	0.0.0.0
priority <integer>	The administrative priority value is used to resolve ties in route selection. In the case where both routes have the same priority, such as equal cost multi-path (ECMP), the IP source hash for the routes will be used to determine which route is selected. The priority range is an integer from 0 to 4294967295. Lower priority routes are preferred routes.	0
weight <integer>	Enter weights for ECMP routes. More traffic is directed to routes with higher weights. This option is available when the `v4-ecmp-mode` field of the `config system settings` command is set to `weight-based`.	0

Example

This example shows how to configure a static route:

```
config router static
   edit 1
      set device mgmt
      set gateway 192.168.0.10
   end
end
```

config switch

Use the `config switch` commands to configure options related to switching functionality:

config switch acl policer

Use this command to configure an ACL policer.

Syntax

```
config switch acl policer
   edit <policer index>
      set description <string>
      set guaranteed-bandwidth <bandwidth_value>
      set guaranteed-burst <in_bytes>
      set maximum-burst <in_bytes>
   end
```

Variable	Description	Default
<policer index>	Enter the index for this ACL policer	No default
description	Enter a text description for the policer.	No default
guaranteed-bandwidth	Enter the amount of bandwidth guaranteed to be available for traffic controlled by the policy. The value range is 0 to 16 776 000 Kbits/second.	0
guaranteed-burst	Guaranteed burst size in bytes (max value = 4294967295)	0
maximum-burst	Maximum burst size in bytes (max value = 4294967295)	0

Example

This example shows how to configure an ACL policer.

```
config switch acl policer
   edit 1
      set description policer1
      set guaranteed-bandwidth 8776000
      set guaranteed-burst 858993459
```

```
      set maximum-burst 4294967295
   end
```

config switch acl policy

Use this command to configure an ACL policy.

Syntax

```
config switch acl policy
edit <policy-id>
   set description <string>
   set ingress-interface <port > [<port > ... <port >]
   set ingress-interface-all {enable | disable}
   config classifier
      set cos <802.1Q CoS value to match>
      set dscp <DSCP value to match>
      set src-mac <mac>
      set dst-mac <mac>
      set ether-type <integer>
      set src-ip-prefix <IP address> <mask>
      set dst-ip-prefix <IP address> <mask>
      set service <service-id>
      set vlan-id <vlan-id>
   end
   config action
      set cos-queue <0 - 7>
      set count {enable | disable}
      set cpu-cos-queue <integer>
      set drop {enable | disable}
      set egress-mask {<physical_port_name> | internal}
      set mirror [internal | <port> | <interface> | <trunk>]
      set outer-vlan-tag <integer>
      set policer <policer>
      set redirect [internal | <port>]
      set redirect-bcast-cpu {enable | disable}
      set redirect-bcast-no-cpu {enable | disable}
      set redirect-physical-port <list of physical ports to redirect>
      set remark-cos <0-7>
      set remark-dscp <0-63>
   end
end
```

Variable	Description	Default
<policy-id>	Enter the unique ID number of this policy.	No default
description	Enter a description or other information about the policy. The description is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces.	No default
ingress-interface	Interface list to which policy is bound on the ingress.	No default

Variable	Description	Default
ingress-interface-all	If enabled, policy is bound to all interfaces.	disable
config classifier		
cos <802.1Q CoS value to match>	Enter the 802.1Q CoS value to match.	No default
dscp <DSCP value to match>	Enter the DSCP value to match.	No default
src-mac	Source MAC address to be matched.	00:00:00:00:00:00
dst-mac	Destination MAC address to be matched.	00:00:00:00:00:00
ether-type	Ether type to be matched.	0x0000
src-ip-prefix	Source IP addresses to be matched.	0.0.0.0 0.0.0.0
dst-ip-prefix	Destination IP addresses to be matched.	0.0.0.0 0.0.0.0
service	Service name to be matched.	No default
vlan-id	VLAN identifier to be matched.	0
config action		
cos-queue <0 - 7>	CoS queue number (0 - 7).	4294967295
count	Enable or disable the **count** action.	disable
cpu-cos-queue <integer>	CPU CoS queue number (20-29). Only if packets reach to CPU. The value range is 20-29.	No default
drop	Enable or disable the **drop** action.	disable
egress-mask {<physical_ port_name> | internal}	List of physical ports to be configured in egress mask.	No default
mirror	Mirror interface name.	No default
outer-vlan-tag	Outer VLAN tag.	0
policer	Identifier of the policer to associate with this policy.	0
redirect	Redirect interface name.	No default
redirect-bcast-cpu	Redirect broadcast to all ports including the CPU.	disable
redirect-bcast-no-cpu	Redirect broadcast to all ports excluding the CPU.	disable

Variable	Description	Default
redirect-physical-port	List of ports to redirect the packet.	No default
remark-cos <0-7>	Set the CoS marking value. The range is 0-7.	No default
remark-dscp <0-63>	Set the DSCP marking value. The range is 0-63.	No default

Examples

In the following example, traffic from VLAN 3 is blocked to a specified destination IP subnet (10.10.0.0/16) but allowed to all other destinations:

```
config switch acl policy
   edit 1
      config action
         set count enable
         set drop enable
      end
      config classifier
         set dst-ip-prefix 10.10.0.0 255.255.0.0
         set vlan-id 3
      end
      set ingress-interface-all enable
   next
   edit 2
      config classifier
         set vlan-id 3
      end
      set ingress-interface-all enable
   next
end
```

In the following example, packets are classified by matching both the CoS and DSCP values. Both the CoS and DSCP marking values are set:

```
config switch acl policy
   edit 1
      config classifier
         set src-mac 11:22:33:44:55:66
         set cos 2
         set dscp 10
      end
      config action
         set count enable
         set remark-cos 4
         set remark-dscp 20
      end
   set ingress-interface port2
```

config switch acl service custom

Use this command to customize one of the ACL services.

Syntax

```
config switch acl service custom
   edit <service name>
      set comment <string>
      set color <0-32>
      set protocol {ICMP | IP | TCP/UDP/SCTP}
      set protocol-number <IP protocol number>
      set sctp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-
          <srcporthigh_int>]
      set tcp-portrange <dstportlow_int>[-<dstporthigh_int>:<srcportlow_int>-<srcporthigh_
          int>]
      set udp-portrange <dstportlow_int>[-<dstporthigh_int>:<srcportlow_int>-<srcporthigh_
          int>]
   end
end
```

Variable	Description	Default
<service name>	Enter the name of this custom service.	No default
comment	Add comments for the custom service.	No default
color	Set the icon color to use in the Web-based manager. A value of zero sets the default color (1).	0
protocol	Select the protocol used by the service. These protocols are available when explicit-proxy is enabled.	TCP/UDP/SCTP
protocol-number	For an IP service, enter the IP protocol number.	0
sctp-portrange	For SCTP services, enter the destination and source port ranges.	No default
tcp-portrange	For TCP services, enter the destination and source port ranges.	No default
udp-portrange	For UDP services, enter the destination and source port ranges.	No default

Notes:

- **srcport_low** and **srcport_high** can be omitted if the value pair is 1-65535
- **dstport_high** can be omitted if **dstport_low** is equal to **dstport_high**
- **srcport_low** and **srcport_high** can be omitted if the value pair is 1-65535
- **dstport_high** can be omitted if **dstport_low** is equal to **dstport_high**

Example

In the following example, Server Message Block (SMB) traffic received on port 1 is mirrored to port 3. SMB protocol uses port 445:

```
config switch acl service custom
   edit "SMB"
      set tcp-portrange 445
   next
end
config switch acl policy # apply policy to port 1 ingress and send to port 3
   edit 1
      set description "cnt_n_mirror_smb"
      set ingress-interface "port1"
      config action
         set count enable
         set mirror "port3"
      end
      config classifier
         set service "SMB"
         set src-ip-prefix 20.20.20.100 255.255.255.255
         set dst-ip-prefix 100.100.100.0 255.255.255.0
      end
   next
end
```

config switch acl settings

Use this command to configure the global ACL settings

Syntax

```
config switch acl settings
   set density-mode {disable | enable}
   set trunk-load-balance {disable | enable}
end
```

Variable	Description	Default
density-mode	Enable or disable density mode.	disable
trunk-load-balance	Enable or disable trunk-load-balancing for ACL actions.	enable

Example

The following example configures the global ACL settings:

```
config switch acl settings
   set density-mode enable
   set trunk-load-balance enable
end
```

config switch flapguard settings

Use this command to configure port flap-guard settings.

Syntax

```
config switch flapguard settings
   set status {disable | enable}
```

```
    set flap-rate <integer>
    set flap-duration <integer>
end
```

Variable	Description	Default
status	Enable or disable flap-guard	disable
flap-rate <integer>	Range is 5-300. Units is seconds.	5
flap-duration <integer>	Range is 5-300. Units is seconds.	30

Example

The following example configures port flap-guard settings:

```
config switch flapguard settings
    set status enable
    set flap-rate 150
    set flap-duration 100
end
```

config switch global

Use this command to configure system-wide FortiSwitch settings.

Syntax

```
config switch global
    set alert-interval <1-1440>
    set auto-fortilink-discovery {enable | disable}
    set auto-isl {enable | disable}
    set auto-isl-port-group <0 - 9>
    set dhcp-snooping-database-export {disable | enable}
    set dmi-global-all {enable | disable}
    set forti-trunk-dmac <xx:xx:xx:xx:xx:xx>
    set ip-mac-binding {enable | disable}
    set log-mac-limit-violations {enable | disable}
    set loop-guard-tx-interval <0 - 30>
    set mac-aging-interval <seconds>
    set max-path-in-ecmp-group <integer>
    set mclag-peer-info-timeout <integer>
    set mclag-stp-aware {enable | disable}
    set name <string>
    set neighbor-discovery-to-cpu {enable | disable}
    set packet-buffer-mode {store-forward | cut-through}
    set poe-alarm-threshold <threshold (percent of total power budget) above which an alarm
        event is generated>
    set poe-power-mode {first-come-first-served | priority}
    set poe-guard-band <integer>
    set poe-pre-standard-detect {disable | enable}
    set poe-power-budget <integer>
    set reserved-mcast-to-cpu {enable | disable}
    set trunk-hash-mode {default| enhanced}
    set trunk-hash-unicast-src-port {enable | disable}
```

```
    set trunk-hash-unkunicast-src-dst
    set virtual-wire-tpid
    config port-security
       set reauth-period <0-1440>
       set mab-reauth {enable | disable}
       set max-reauth-attempt <0-15>
       set link-down-auth {no-action | set-unauth}
    end
end
```

Variable	Description	Default
alert-interval <1-1440>	Set how often an alert is generated for temperature and PoE sensors when they exceed their set thresholds.	10
auto-fortilink-discovery	Enable or disable the capability for FortiGate to automatically discover the FortiLink interface on the switch.	enable
auto-isl	Enable or disable the capability to automatically form an inter-switch LAG.	enable
auto-isl-port-group	Set the ISL port group. Range is 0-9.	0
dhcp-snooping-database-export {disable | enable}	Enable or disable whether the DHCP snooping database is exported to file.	disable
dmi-global-all	Enable or disable DMI globally.	enable
forti-trunk-dmac <xx:xx:xx:xx:xx:xx>	Enter the destination MAC address to be used for FortiTrunk heartbeat packets.	02:80:c2:00:00:02
ip-mac-binding	Enable or disable IP-MAC binding for the switch	disable
log-mac-limit-violations {enable | disable}	Enable or disable the logging of layer-2 learning limit violations for an interface or VLAN.	disable
loop-guard-tx-interval	Enter the loop guard transmit interval. Value range is 1-30. The units is seconds.	3
mac-aging-interval <seconds>	Set the time period after which an unused MAC address is removed from the MAC table. Range 10 to 1,000,000 seconds. 0 disables.	300
max-path-in-ecmp-group <integer>	Set the maximum path in one ECMP group.	8
mclag-peer-info-timeout <integer>	Enter the MCLAG peer info timeout. The value range is 30 to 600 seconds.	30

Variable	Description	Default
mclag-stp-aware {enable | disable}	Enable or disable whether the STP can be used within the MCLAG.	enable
name <string>	Enter a name for the switch.	No default
neighbor-discovery-to-cpu {enable | disable}	Enable or disable the forwarding of reserved multicast packets to the CPU. Applies only to the 124D, 124D-POE, 200 Series, and 400 Series.	enable
packet-buffer-mode {store-forward | cut-through}	Set the switching mode to store-and-forward or cut-through for the main buffer of the FSW-1024D, FSW-1048D, or FSW-3032D model.	store-forward
poe-alarm-threshold <threshold (percent of total power budget) above which an alarm event is generated>	Enter the threshold (a specified percentage of the total power budget) above which an alarm event is generated.	80
poe-power-mode {first-come-first-served | priority}	Set the PoE power mode to priority based or first-come, first-served.	priority
poe-guard-band <integer>	Enter the power (W) to reserve in case of a spike in PoE consumption.	19
poe-pre-standard-detect {disable | enable}	Enable or disable PoE pre-standard detection.	enable
poe-power-budget <integer>	Set or override the maximum power budget.	400
reserved-mcast-to-cpu {enable | disable}	Enable or disable the forwarding of IPv6 neighbor-discovery packets to the CPU. Applies only to the 124D, 124D-POE, 200 Series, and 400 Series.	enable
trunk-hash-mode	Set the trunk hash mode to default or enhanced	default
trunk-hash-unicast-src-port {enable | disable}	Enable or disable whether the trunk hashing algorithm for unicast packets uses the source port.	disable
trunk-hash-unkunicast-src-dst	Enable or disable trunk hash for unknown unicast src-dst.	enable
virtual-wire-tpid	TPID value used by virtual-wires. The value from 0x0001 to 0xfffe Choose a value unlikely to be seen as a TPID or ethertype in your network.	0xdee5
config port-security		

Variable	Description	Default
reauth-period	Defines how often the device needs to reauthenticate. If a session remains active beyond this number of minutes, the system requires the device to reauthenticate. Set the value to 0 to disable reauthentication.	60
mab-reauth {enable | disable}	Enable or disable whether MAB retries authentication before assigning a device to a guest VLAN for unauthorized users.	disable
max-reauth-attempt	If 802.1x authentication fails, this setting caps the number of reattempts that the system will initiate.	2
link-down-auth	If a link goes down, this setting determines if the affected devices needs to reauthenticate. • `set-unauth` — revert all devices to the un-authenticated state. Each device will need to reauthenticate. • `no-action` — if reauthenication is not required.	set-unauth

Example

The following example configures system-wide FortiSwitch settings:

```
config switch global
   set auto-isl enable
   set dhcp-snooping-database-export enable
   set dmi-global-all enable
   set ip-mac-binding enable
   set loop-guard-tx-interval 15
   set mac-aging-interval 150
   set max-path-in-ecmp-group 4
   set mclag-peer-info-timeout 300
   set poe-alarm-threshold 40
   set poe-power-mode first-come-first-served
   set poe-guard-band 10
   set poe-pre-standard-detect enable
   set poe-power-budget 200
   set trunk-hash-mode enhanced
   set trunk-hash-unkunicast-src-dst enable
end
```

config switch igmp-snooping globals

Use this command to configure IGMP snooping on the FortiSwitch.

Syntax

```
config switch igmp-snooping globals
   set aging-time <integer>
   set flood-unknown-multicast {enable | disable}
```

```
   set query-interval <10-1200>
end
```

Variable	Description	Default
aging-time	max number of seconds to retain a multicast snooping entry for which no packets have been seen (15-3600)	300
flood-unknown-multicast	Enable or disable whether to flood the vlan with unknown multicast messages	disable
query-interval <10-1200>	Enter the maximum number of seconds between IGMP queries.	120

Example

The following example configures IGMP snooping on the FortiSwitch:

```
config switch igmp-snooping globals
   set aging-time 150
   set flood-unknown-multicast enable
   set query-interval 200
end
```

config switch interface

Use this command to configure FortiSwitch features on an interface.

Command

```
config switch interface
   edit <interface_name>
      set allowed-vlans {vlan1 vlan2 ...}
      set arp-inspection-trust {trusted | untrusted}
      set auto-discovery-fortilink {enable | disable}
      set auto-discovery-fortilink-packet-interval <3-300>
      set default-cos <0 - 7>
      set discard-mode {all-tagged | all-untagged | none}
      set dhcp-snooping {trusted | untrusted}
      set dhcp-snoop-learning-limit-check {disable | enable}
      set dhcp-snooping-option82-trust {enable | disable}
      set edge-port {enabled | disabled}
      set igmp-snooping {allowed | not-allowed}
      set igmps-flood-reports {enable | disable}
      set igmps-flood-traffic {enable | disable}
      set ip-mac-binding {enable | disable | global}
      set learning-limit <1 - 128>
      set loop-guard {enable | disable}
      set native-vlan <vlan_int>
      set private-vlan {disabled | promiscuous sub-vlan}
      set qos-policy {<string> | default}
      set sflow-sampler {enable | disable}
      set snmp-index <integer>
      set sticky-mac {disable | enable}
```

```
        set stp-bpdu-guard {disabled | enabled}
        set stp-loop-protection {enabled | disabled}
        set stp-root-guard {disabled | enabled}
        set stp-state {enabled | disabled}
        set trust-dot1p-map <string>
        set trust-ip-dscp-map <string>
        set untagged-vlans {vlan1 vlan2 ...}
        config port-security
           set port-security-mode {none | 802.1X | 8021X-mac-based}
           set mac-auth-bypass {enable | disable}
           set guest-vlan {enable | disable}
           set guest-vlanid <VLAN_id>
           set guest-auth-delay <integer>
           set auth-fail-vlan {enable | disable}
           set auth-fail-vlanid <VLAN_id>
           set eap-passthru {disable | enable}
           set radius-timeout-overwrite {enable | disable}
        end
        set security-groups <security-group-name>
    end
```

Variable	Description	Default
<interface_name>	Enter the name of the interface.	No default
allowed-vlans {vlan1 vlan2 ...}	Enter the names of the VLANs permitted on this interface.	No default
arp-inspection-trust {trusted | untrusted}	Set the interface to trusted or untrusted.	untrusted
auto-discovery-fortilink {enable | disable}	Enable or disable automatically discovery of the port used for FortiLink.	disable
auto-discovery-fortilink-packet-interval <3-300>	Enter the FortiLink packet interval for automatic discovery. The value range is 3 to 300 seconds.	5
default-cos <0 - 7>	Set the default CoS value for untagged packets. Integer in the range of 0 to 7. The configured default CoS only applies if you also set **trust-dot1p-map** on the interface.	0
discard-mode {all-tagged | all-untagged | none}	Set the discard mode for this interface.	none
dhcp-snooping {trusted | untrusted}	Set the interface to trusted or untrusted.	untrusted
dhcp-snoop-learning-limit-check {disable | enable}	Enable or disable whether there is a limit for how many IP addresses are in the DHCP snooping binding database for this interface.	disable

Variable	Description	Default
dhcp-snooping-option82-trust {enable | disable}	Enable or disable (allow/disallow) DHCP packets with option-82 on an untrusted interface.	disable
edge-port {enabled | disabled}	Enable if the port does not have another switch connected to it.	disable
igmp-snooping {allowed | not-allowed }	Allow or disallow this interface from taking part in IGMP snooping.	not-allowed
igmps-flood-reports {enable | disable}	Enable or disable whether to flood IGMP reports to this interface.	enable
igmps-flood-traffic {enable | disable}	Enable or disable whether to flood multicast traffic to this interface.	disable
ip-mac-binding {enable | disable | global}	Enable or disable IP-MAC binding for this interface. Set the value to 'global', the interface inherits the global ip-mac-binding configuration value.	disable
learning-limit <1 - 128>	Limit the number of dynamic MAC addresses on this port. The value range is between 0 and 128 (0 = no limit).	0
loop-guard {enable | disable}	Enable or disable loop guard for this interface.	disable
native-vlan <vlan_int>	Enter the native (untagged) VLAN for this interface.	1
private-vlan {disabled | promiscuous | sub-vlan}	Enable private VLAN functionality. **Note:** Private VLANs are not supported on the FortiSwitch-28C.	disabled
qos-policy {<string> | default}	Enter the name of the QoS egress CoS queue policy.	default
sflow-sampler {enable | disable}	Enable or disable the sFlow protocol on this interface	disable
snmp-index <integer>	Enter the SNMP index for this interface.	Default is the port number
sticky-mac {disable | enable}	Enable or disable whether dynamically learned MAC addresses are persistent when the status of a FortiSwitch port changes (goes down or up).	disable
stp-bpdu-guard {disabled | enabled}	Enable or disable STP BPDU guard protection. To use STP BPDU guard on this interface, you must enable stp-state and edge-port.	disabled
stp-loop-protection {enabled | disabled}	Enable or disable STP loop protection on this interface.	disabled

Variable	Description	Default
stp-root-guard {disabled | enabled}	Enable or disable STP root guard protection. To use STP root guard, you must enable stp-state.	disabled
stp-state {enabled | disabled}	Enable or disable Spanning Tree Protocol (STP) on this interface.	enabled
trust-dot1p-map	Whether to trust the dot1p CoS value in the incoming packets. Specify a map to map the CoS value to an egress queue value.	No default
trust-ip-dscp-map	Whether to trust the DSCP QoS value in the incoming packets. Specify a map to map the DSCP value to an egress queue value.	No default
untagged-vlans	Select the allowed-vlans to be transmitted without VLAN tags	No default
config port-security		
port-security-mode {none | 802.1X | 8021X-mac-based}	Set the security mode for the port. Set the security mode to `802.1X` for port-based authentication or `802.1Xmac-based` for MAC-based authentication. If you change the security mode from `none`, you must set the security group with the `set security-groups` command.	none
mac-auth-bypass {enable | disable}	Enable or disable MAC auth bypass.	disable
guest-vlan {enable | disable}	When enabled, the system assigns the **guest-vlanid** to unauthorized users.	disable
guest-vlanid <VLAN_id>	VLAN identifier. Mandatory field when guest VLAN is enabled.	100
guest-auth-delay <integer>	If a device does not attempt to authenticate within this timeframe, the guest VLAN is assigned.	30
auth-fail-vlan {enable | disable}	When enabled, the system assigns the **auth-fail-vlanid** to users who attempted to authenticate but failed to provide valid credentials.	disable
auth-fail-vlanid <VLAN_id>	VLAN identifier. Mandatory field when auth-fail VLAN is enabled.	200
eap-passthru {disable | enable}	Enable or disable the EAP pass-through mode.	disable

Variable	Description	Default
radius-timeout-overwrite {enable | disable}	Enable or disable whether to use the RADIUS-provided re-authentication timeout. If the setting is enabled, the port uses the local timeout.	disable
security-groups <security-group-name>	Enter the security group name if you are using port-based authentication or MAC-based authentication.	No default

Example

The following example shows QoS configuration on a trunk interface:

```
config switch interface
   edit "tr1"
      set snmp-index 56
      set trust-dot1p-map "dot1p_map1"
      set default-cos 1
      set qos-policy "p1"
   next
end
```

config switch ip-mac-binding

Use IP-MAC binding to prevent ARP spoofing.

The port accepts a packet only if the source IP address and source MAC address in the packet match an entry in the IP-MAC binding table.

You can enable or disable IP-MAC binding for the whole switch, and you can override this global setting for each port.

Syntax

```
config switch ip-mac-binding
   edit <sequence_int>
      set ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
      set mac <xx:xx:xx:xx:xx:xx>
      set status {enable | disable}
   next
end
```

Variable	Description	Default
<sequence_int>	Enter a sequence number for the IP-MAC binding entry.	No default
ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the source IP address and network mask for this rule.	0.0.0.0 0.0.0.0
mac <xx:xx:xx:xx:xx:xx>	Enter the MAC address for this rule.	00:00:00:00:00:00
status {enable | disable}	Enable or disable the IP-MAC binding.	disable

Example

The following example configures the IP-MAC binding for the FortiSwitch:

```
config switch ip-mac-binding
   edit 1
      set ip 172.168.20.1 255.255.255.255
      set mac 00:21:cc:d2:76:72
      set status enable
   next
end
```

config switch lldp profile

Use this command to configure LLDP profile settings. The LLDP profile contains most of the port-specific configuration. Profiles are designed to provide a central point of configuration for LLDP settings that are likely to be the same for multiple ports.

There are two static LLDP profiles: **default** and **default-auto-isl**. These profiles are created automatically. They can be modified but cannot be deleted. The **default-auto-isl** profile always has auto-isl enabled, and rejects any configurations which attempt to disable it.

Syntax

```
config switch lldp profile
   edit <profile>
      set 802.1-tlvs port-vlan-id
      set 802.3-tlvs max-frame-size
      set auto-isl {enable | disable}
      set auto-isl-hello-timer <1-30>
      set auto-isl-port-group <0-9>
      set auto-isl-receive-timeout <3-90>
      set med-tlvs (inventory-management | network-policy)
      config custom-tlvs
         edit <TLVname_str>
            set information-string <hex-bytes>
            set oui <hex-bytes>
            set subtype <integer>
         end
      config med-network-policy
         edit {guest-voice |  guest-voice-signaling | softphone-voice |
            streaming-video | video-conferencing | video-signaling |
            voice | voice-signaling}
            set status {enable | disable}
            set dscp <0 - 63>
            set priority <0 - 7>
            set vlan <0 - 4094>
         end
```

Variable	Description	Default
profile	Enter a name for the LLDP profile.	No default

Variable	Description	Default
802.1-tlvs	The only 802.1 TLV that can be enabled or disabled is **port-vlan-id**. This TLV will send the native VLAN of the port. If the value is changed, the sent value will reflect the updated value.	no TLV enabled
802.3-tlvs	The only 802.3 TLV that can be enabled or disabled is **max-frame-size**. This TLV will send the maximum frame size value of the port. If the value is changed, the sent value will reflect the updated value.	no TLV enabled
auto-isl	Enable or disable the auto ISL capability.	Disabled
auto-isl-hello-timer <1-30>	Enter a value (in seconds) for the hello timer. The range is 1 to 30.	3
auto-isl-port-group <0-9>	Enter a value for the port group. The range is 0 to 9.	0
auto-isl-receive-timeout	Enter a value (in seconds) for the receive timeout. The range is 3 to 90.	9
med-tlvs (inventory-management | network-policy)	enable the Inventory Management TLVs and/or the Network Policy TLVs.	**inventory-management** and **network-policy**
config custom-tlvs		
<TLVname_str>	Enter the TLV name.	No default
information-string	Organizationally defined information string. Enter up to 507 bytes in hexadecimal notation.	No default
oui	Organizationally unique identifier. Enter 3 hexadecimal bytes (000000 - FFFFFF). At least one byte must have a non-zero value.	000000
subtype	Organizationally defined subtype. Enter an integer in the range of 0 to 255.	0
config med-network-policy		
{guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling}	Enter one of the policy type names.	No default
status	Enable or disable the policy for the policy type.	Disabled

Variable	Description	Default
dscp	DSCP value to send. Range is 0 to 63.	0
priority	CoS priority value to send. Range is 0 to 7.	0
vlan	VLAN value to send. Range is 0 to 4094.	0

Note: LLDP-MED network policies cannot be deleted or added. To use a policy, the **med-tlvs** field must include **network-policy**, and you must set the policy to **enabled**. The VLAN values on the policy are cross-checked against the VLAN native, allowed, and untagged attributes for any interfaces that contain physical-ports using this profile. The cross-check determines if the policy TLV should be sent (VLAN must be native or allowed), and if the TLV should mark the VLAN as tagged or untagged (VLAN is native, or is in untagged). The network policy TLV is automatically updated when a switch interface changes VLAN configuration, or if a physical port is added to, or removed from, a trunk.

Example

The following example configures an LLDP-MED profile:

```
config switch lldp profile
   edit "Forti670i"
      config med-network-policy
         edit "voice"
            set dscp 46
            set priority 5
            set status enable
            set vlan 400
         next
         edit "guest-voice"
         next
         edit "guest-voice-signaling"
         next
         edit "softphone-voice"
         next
         edit "video-conferencing"
         next
         edit "streaming-video"
            set dscp 40
            set priority 3
            set status enable
            set vlan 400
         next
         edit "video-signaling"
         next
      end
   set med-tlvs inventory-management network-policy
next
end
```

config switch lldp settings

Configure the global LLDP settings.

Syntax

```
config switch lldp settings
   set status {enable| disable}
   set tx-hold <1-16>
   set tx-interval <5-4095>
   set fast-start-interval <0 or 2-5>
   set management-interface (internal | <string>)
end
```

Variable	Description	Default
status	Enable or disable	Enabled
tx-hold	Number of tx-intervals before the local LLDP data expires. Therefore, the packet TTL (in seconds) is **tx-hold** times **tx-interval**. The range for tx-hold is 1 to 16.	4
tx-interval	How often the FortiSwitch transmits the LLDP PDU. The range is 5 to 4095 seconds.	30
fast-start-interval	How often the FortiSwitch transmits the first 4 LLDP packets when a link comes up. The range is 2 to 5 seconds. Set this variable to zero to disable fast start.	2
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	**mgmt** or **internal**, depending on FortiSwitch model.

Example

The following example configures the global LLDP settings:

```
config switch lldp settings
   set status enable
   set tx-hold 8
   set tx-interval 2000
   set fast-start-interval 3
   set management-interface internal
end
```

config switch mirror

Use this command to configure the port mirror.

Syntax

```
config switch mirror
   edit <mirror name>
      set dst <interface>
      set status {active | inactive}
```

```
      set switching-packet {enable | disable}
   end
```

Variable	Description	Default
<mirror name>	Enter the mirror to be configured (or a new mirror name)	No default
dst <interface>	Enter the port that will act as a mirror.	No default
status {active | inactive}	Set mirroring to active or inactive.	inactive
switching-packet {enable | disable}	Enable or disable switching functionality when mirroring.	disable

Example

The following example configures a port mirror:

```
config switch mirror
   edit "m1"
      set dst "port5"
      set src-egress "port2" "port3"
      set src-ingress "port2" "port4"
      set status active
      set switching-packet enable
   end
```

config switch network-monitor directed

Use this command to configure a static entry for network monitoring on the FortiSwitch.

Syntax

```
config switch network-monitor directed
   edit <unused network monitor>
      set monitor-mac <xx:xx:xx:xx:xx:xx>
   end
```

Variable	Description	Default
<unused network monitor>	Enter the number of an unused network monitor.	No default
monitor-mac <xx:xx:xx:xx:xx:xx>	Enter the MAC address to be monitored.	00:00:00:00:00:00

Example

The following example specifies a MAC address to be monitored:

```
config switch network-monitor directed
   edit 1
      set monitor-mac 00:25:00:61:64:6d
   next
end
```

config switch network-monitor settings

Use this command to configure global settings for network monitoring on the FortiSwitch.

Syntax

```
config switch network-monitor settings
   set db-aging-interval <integer>
   set status {disable | enable}
   set survey-mode {disable | enable}
   set survey-mode-interval <integer>
end
```

Variable	Description	Default
db-aging-interval <integer>	Enter the network monitor database aging interval. The value range is 3600-86400 seconds. Set the option to 0 to disable it.	3600
status {disable | enable}	Enable or disable the network monitor.	disable
survey-mode {disable | enable}	Enable or disable the network monitor survey mode.	disable
survey-mode-interval <integer>	Enter the duration for which a network monitor is programmed in hardware in the survey mode. The value range is 120-3600 seconds.	120

Example

The following example starts network monitoring in survey mode:

```
config switch network-monitor settings
   set status enable
   set survey-mode enable
   set survey-mode-interval 480
end
```

config switch phy-mode

On FortiSwitch models that provide 40G QSFP (quad small form-factor pluggable) interfaces, you can install a breakout cable to convert one 40G interface into four 10G interfaces. Use this command to configure split ports.

Notes

- Split port is supported on the following FortiSwitch models:
  - 3032D (ports 5 to 28 are splittable)
  - 524D, 524D-FPOE (ports 29 and 30 are splittable)
  - 548D, 548D-FPOE (ports 53 and 54 are splittable)
- Currently, the maximum number of ports supported in software is 64. Therefore, only 10 QSFP ports can be split. This limitation applies to all of the models, but only the 3032D has enough ports to encounter this limit.
- Split port is not supported in FortiLink mode (that is, FortiSwitch managed by FortiGate).

Syntax

```
config switch phy-mode
   set port-configuration <default | disable-port54 | disable-port41-48>
   set port<number>-phy-mode {1x40G | 4x10G}
   ...
end
```

NOTE: The port-configuration command applies only to the 548D and 548D-FPOE models.

Variable	Description	Default
port-configuration <default | disable-port54 | disable-port41-48>	Set this option to `disable-port54` if only port 53 is splittable and port 54 is unavailable. Set this option to `disable-port41-48` if ports 41 to 48 are unavailable, but ports 53 and 54 are splittable.	default
port<number>-phy-mode {1x40G | 4x10G}	Set the specified port to one 40G interface or four 10G interfaces. Use one entry for each port that supports split ports.	1x40G

Example

In the following example, a FortiSwitch 3032D is configured with ports 10, 14, and 28 set to 4x10G:

```
config switch phy-mode
   set port5-phy-mode 1x40G
   set port6-phy-mode 1x40G
   set port7-phy-mode 1x40G
   set port8-phy-mode 1x40G
   set port9-phy-mode 1x40G
   set port10-phy-mode 4x10G
   set port11-phy-mode 1x40G
   set port12-phy-mode 1x40G
   set port13-phy-mode 1x40G
   set port14-phy-mode 4x10G
   set port15-phy-mode 1x40G
   set port16-phy-mode 1x40G
   set port17-phy-mode 1x40G
   set port18-phy-mode 1x40G
   set port19-phy-mode 1x40G
   set port20-phy-mode 1x40G
   set port21-phy-mode 1x40G
   set port22-phy-mode 1x40G
   set port23-phy-mode 1x40G
   set port24-phy-mode 1x40G
   set port25-phy-mode 1x40G
   set port26-phy-mode 1x40G
   set port27-phy-mode 1x40G
   set port28-phy-mode 4x10G
end
```

config switch physical-port

Use this command to configure a physical port.

Syntax

```
config switch physical-port
   edit <port_name>
      set cdp-status {disable | rx-only | tx-only | tx-rx}
      set description <description_str>
      set dmi-status {disable | enable | global}
      set egress-drop-mode {disabled | enabled>
      set flow-control {tx | rx | both | disable}
      set l2-learning {enable | disable}
      set lldp-status {tx-only | rx-only | tx-rx | disable}
      set lldp-profile <profile name>
      set max-frame-size <bytes_int>
      set poe-port-mode {IEEE802_3AF | IEEE802_3AT}
      set poe-port-priority {critical-priority | high-priority | low-priority}
      set poe-status {enable | disable}
      set qsfp-low-power-mode {enabled | disabled}
      set speed <speed_str>
      set status {down | up}
   end
```

Variable	Description	Default
<port_name>	Enter the port name.	No default
cdp-status {disable | rx-only | tx-only | tx-rx}	Set the CDP transmit and receive status (LLDP must be enabled in LLDP settings). • `disable` disables CDP transmit and receive. • `rx-only` enables CDP as receive only. • `tx-only` enables CDP as transmit only. • `tx-rx` enables CDP transmit and receive.	disable
description <description_str>	Optionally enter a description.	No default
dmi-status	Enable or disable DMI access. Set to `global` to use the global switch setting.	global
egress-drop-mode {disabled | enabled>	Enable or disable egress drop.	enabled
flow-control {tx | rx | both | disable}	Set flow control: • `tx` — enable transmit pause only • `rx` — enable receive pause only • `both` — enable both transmit and receive pause • `disable` — disable flow control	disable

Variable	Description	Default
l2-learning	Enable or disable dynamic IP learning for this interface	enabled
lldp-status	Set LLDP status for this port: `tx-only` — enable transmit only `rx-only` — enable receive only `tx-rx` — enable both transmit and receive `disable` — disable LLDP	tx-rx
lldp-profile	Enter the LLDP profile name for this port.	default
max-frame-size <bytes_int>	Set the maximum frame size. Range 68 to 16360.	9216
poe-port-mode {IEEE802_3AF | IEEE802_3AT}	Set the PoE port mode to IEEE802.3AFor IEEE802.3AT.	IEEE802_3AT
poe-port-priority {critical-priority | high-priority | low-priority}	Set the port priority.	low-priority
poe-status {enable | disable}	Enable Power over Ethernet. This option is only available with the FortiSwitch-324B-POE.	enable
qsfp-low-power-mode {enabled | disabled}	Enable or disable the low-power mode on FortiSwitch models with QSFP (quad small form-factor pluggable) ports.	disabled
speed <speed_str>	Set the speed of this port: • `1000auto`—Auto-negotiation (1G bps full-duplex only). • `100full`—100 Mbps full-duplex. • `100half`—100 Mbps half-duplex. • `10full`—10 Mbps full-duplex. • `10half`—10 Mbps half-duplex. • `auto`—Auto-negotiation.	auto
status {down | up}	Set the administrative status of this interface: `up` or `down`.	up

Example

In the following example, port 4 is configured:

```
config switch physical-port
   edit "port4"
      set lldp-profile "Forti670i"
      set speed auto
   next
end
```

config switch qos dot1p-map

Use this command to configure a dot1p map. A dot1p map defines a mapping between IEEE 802.1p CoS values (from incoming packets on a trusted interface) and the egress queue values.

Syntax

```
config switch qos dot1p-map
   edit <dot1p map name>
      set description <text>
      set [priority-0|priority-1|priority-2|...priority-7] <queue number>
   next
end
```

Variable	Description	Default
<dot1p map name>	Enter the name of a dot1p map.	No default
<text>	Enter a description of the dot1p map.	No default
[priority-0|priority-1|priority-2|...priority-7] <queue number>	Set the priority of each queue.	queue-0

Example

```
config switch qos dot1p-map
   edit "test1"
      set priority-0 queue-2
      set priority-1 queue-0
      set priority-2 queue-1
      set priority-3 queue-3
      set priority-4 queue-4
      set priority-5 queue-5
      set priority-6 queue-6
      set priority-7 queue-7
   next
end
```

Values that are not explicitly included in the map will follow the default mapping, which maps each priority (0-7) to queue 0.

If an incoming packet contains no CoS value, the switch assigns a CoS value of zero. Use the **set default-cos** interface command to configure a different default CoS value. The valid range is from 0 to 7. The configured default CoS only applies if you also set **trust-dot1p-map** on the interface.

config switch qos ip-dscp-map

Use this command to configure a DSCP map. A DSCP map defines a mapping between IP Precedence or Differentiated Services Code Point (DSCP) values and the egress queue values.

Syntax

```
config switch qos ip-dscp-map
   edit <ip-dscp map name>
      set description <text>
      config map
         edit <entry-name>
            set diffserv [ [ AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 |
                AF41 | AF42 | AF43 | CS0 | CS1 | CS2 | CS3 | CS4 | CS5 | CS6 | CS7 | EF ]
            set ip-precedence [ Network Control | Internetwork Control | Critic/ECP | Flash
                Override | Flash, Immediate | Priority | Routine ]
            set value <dscp raw value>
            set cos-queue <queue number>
         next
      end
   next
end
```

Variable	Description	Default
<ip-dscp map name>	Enter the name of a DSCP map.	No default
<text>	Enter a description of the DSCP map.	No default
<entry-name>	Enter a unique integer to create a new entry.	No default
diffserv [[AF11 | AF12 | AF13 | AF21 | AF22 | AF23 | AF31 | AF32 | AF33 | AF41 | AF42 | AF43 | CS0 | CS1 | CS2 | CS3 | CS4 | CS5 | CS6 | CS7 | EF]	Set the differentiated service.	No default
ip-precedence [Network Control | Internetwork Control | Critic/ECP | Flash Override | Flash, Immediate | Priority | Routine]	Set the IP precedence.	No default
value <dscp raw value>	enter the raw value of DSCP (0 - 63).	No default
cos-queue <queue number>	Enter the CoS queue number.	0

Example

The following example defines a mapping for two of the DSCP values:

```
config switch qos ip-dscp-map
   edit "m1"
      config map
         edit "e1"
            set cos-queue 0
            set ip-precedence Immediate
         next
         edit "e2"
            set cos-queue 3
```

```
            set value 13
        next
    end
  next
end
```

Values that are not explicitly included in the map will follow the default mapping, which assigns queue 0 for all DSCP values.

config switch qos qos-policy

Use this command to configure QoS policies.

In a QoS policy, you set the scheduling mode (Strict, Round Robin, Weighted Round Robin) for the policy, and configure one or more CoS queues.

Syntax

```
config switch qos qos-policy
  edit <policy_name>
    set schedule [ strict | round-robin | weighted ]
    config cos-queue
      edit [queue-0 ... queue-7]
        set description <text>
        set min-rate <rate kbps>
        set max-rate <rate kbps>
        set drop-policy {taildrop | weighted-random-early-detection}
        set weight <value>
        set wred-slope <value>
      next
    end
  next
end
```

Variable	Description	Default
<policy_name>	Enter the name of the QoS policy.	No default

Variable	Description	Default
schedule [strict | round-robin | weighted]	Set the CoS queue scheduling. • strict — The queues are served in descending order (of queue number), so higher number queues receive higher priority. The purpose of the strict scheduling mode is to provide lower latency service to higher classes of traffic. However, if the interface experiences congestion, the lower priority traffic could be starved. • round-robin — In round robin mode, the scheduler visits each backlogged queue, servicing a single packet from each queue before moving on to the next one. The purpose of round robin scheduling is to provide fair access to the egress port bandwidth. • weighted — Each of the eight egress queues is assigned a weight value ranging from 0 to 63. The purpose of weighted round robin scheduling is to provide prioritized access to the egress port bandwidth, such that queues with higher weight get more of the bandwidth, but lower priority traffic is not starved.	round-robin
[queue-0 … queue-7]	Set the CoS queue to update.	No default
description <text>	Enter a description of the CoS queue.	No default
min-rate <rate kbps>	Enter the minimum rate in kbps. Set the value to 0 to disable.	0
max-rate <rate kbps>	Enter the maximum rate in kbps. Set the value to 0 to disable.	0
drop-policy {taildrop | weighted-random-early-detection}	Set the CoS queue drop policy. • taildrop — When the queue is full, new packets are dropped. • weighted-random-early-detection — When the queue is full, lower priority packets are dropped.	taildrop
weight <value>	Enter the weight of weighted round robin scheduling. (applicable if the policy schedule is weighted)	1
wred-slope <value>	Enter the slope of WRED drop probability.	45

Example

The following example defines a QoS policy for queue 0:

```
config switch qos qos-policy
   edit policy1
```

```
set schedule weighted
config cos-queue
   edit queue-0
      set description "QoS policy for queue 0"
      set min-rate 10
      set max-rate 20
      set drop-policy weighted-random-early-detection
      set weight 5
      set wred-slope 15
   end
end
```

config switch security-feature

Use this command to configure security checks for incoming TCP/UDP packets. The packet is dropped if the system detects the specified condition.

Syntax (for models FS108D-POE, FS112D-POE, FS224D-POE)

```
config switch security-feature
   set tcp-syn-data {enable | disable}
   set tcp-udp-port-zero {enable | disable}
   set tcp_flag_zero {enable | disable}
   set tcp_flag_FUP {enable | disable}
   set tcp_flag_SF {enable | disable}
   set tcp_flag_SR {enable | disable}
   set tcp_frag_ipv4_icmp {enable | disable}
   set tcp_arp_mac_mismatch {enable | disable}
end
```

Variable	Description	Default
tcp-syn-data	TCP SYN packet contains additional data (possible DoS attack).	disable
tcp-udp-port-zero	TCP or UDP packet has source or destination port set to zero.	disable
tcp_flag_zero	TCP packet with all flags set to zero.	disable
tcp_flag_FUP	TCP packet with FIN, URG and PSH flag set.	disable
tcp_flag_SF	TCP packet with SYN and FIN flag set.	disable
tcp_flag_SR	TCP packet with SYN and RST flag set.	disable
tcp_frag_ipv4_icmp	Fragmented ICMPv4 packet.	disable
tcp_arp_mac_mismatch	ARP packet with MAC source address mismatch between the Layer 2 header and the ARP packet payload.	disable

Syntax (for all other models)

```
config switch security-feature
   set sip-eq-dip {enable | disable}
   set tcp-flag {enable | disable}
```

```
    set tcp-port-eq {enable | disable}
    set tcp-flag-FUP {enable | disable}
    set tcp-flag-SF {enable | disable}
    set v4-first-frag {enable | disable}
    set udp-port-eq {enable | disable}
    set tcp-hdr-partial {enable | disable}
    set macsa-eq-macda {enable | disable}
    set allow-mcast-sa {enable | disable}
    set allow-sa-mac-all-zero {enable | disable}
end
```

Variable	Description	Default
sip-eq-dip	TCP packet with a source IP address equal to the destination IP address.	disable
tcp_flag	DoS attack checking for TCP flags.	disable
tcp-port-eq	TCP packet with source and destination TCP ports equal.	disable
tcp-flag-FUP	TCP packet with FIN, URG and PSH flags set, and sequence number is zero.	disable
tcp-flag-SF	TCP packet with SYN and FIN flag set.	disable
v4-first-frag	DoS attack checking for IPv4 first fragment.	disable
udp-port-eq	IP packet with source and destination UDP ports equal.	disable
tcp-hdr-partial	TCP packet with partial header.	disable
macsa-eq-macda	Packet with source MAC address equal to destination MAC address.	disable
allow-mcast-sa	Ethernet packet whose source MAC address is multicast.	enable
allow-sa-mac-all-zero	Ethernet packet whose source MAC address is all zeros.	enable

Example

The following example configures security checks for incoming TCP/UDP packets:

```
config switch security-feature
    set sip-eq-di enable
    set tcp-flag enable
    set tcp-port-eq enable
    set tcp-flag-FUP enable
    set tcp-flag-SF enable
    set v4-first-frag enable
    set udp-port-eq enable
    set tcp-hdr-partial enable
    set macsa-eq-macda enable
    set allow-mcast-sa disable
    set allow-sa-mac-all-zero disable
```

```
end
```

config switch static-mac

Use this command to configure one (or more) static MAC address on an interface.

Syntax

```
config switch static-mac
   edit <sequence number>
      set description <optional_string>
      set interface <interface_name>
      set mac <static_MAC_address>
      set type {sticky | static}
      set vlan-id <1-4095>
   end
```

Variable	Description	Default
<sequence number>	Enter a sequence number.	No default
description <optional_string>	Optional. Enter a description of the static MAC address.	No default
interface <interface_name>	Enter the interface name.	No default
mac <static_MAC_address>	Enter the static MAC address.	00:00:00:00:00:00
type {sticky | static}	Set the MAC address as a persistent (sticky) addres or a static address.	static
vlan-id <1-4095>	Enter the VLAN identifier.	1

Example

```
config switch static-mac
   edit 1
      set description "first static MAC address"
      set interface port10
      set mac d6:dd:25:be:2c:43
      set type static
      set vlan-id 10
   end
```

config switch storm-control

Use this command to configure storm control.

Syntax

```
config switch storm-control
   set broadcast {enable | disable}
   set rate [0 | 1-100000]
   set unknown-multicast {enable | disable}
```

```
set unknown-unicast {enable | disable}
```

Variable	Description	Default
broadcast	Enable or disable storm control for broadcast traffic.	disable
rate [0 | 1-100000]	Specify the rate as packets-per-second. If you set the rate to zero, the system drops all packets (for the enabled traffic types).	0
unknown-multicast	Enable or disable storm control for unknown multicast traffic.	disable
unknown-unicast {enable | disable}	Enable or disable storm control for unknown unicast traffic.	disable

Example

```
config switch storm-control
   set broadcast enable
   set rate 1000
   set unknown-multicast enable
   set unknown-unicast enable
end
```

config switch stp instance

Use this command to configure an STP instance.

Syntax

```
config switch stp instance
   edit <instance_id>
      set priority <priority_int>
      set vlan-range <vlan_map>
      config stp-port
         edit <port name>
            set cost <cost_int>
            set priority <priority_int>
      end
   end
```

Variable	Description	Default
<instance_id>	Enter a number to identify the table entry.	No default
priority <priority_int>	Set the STP priority. The acceptable priority values are 0, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 4096, 40960, 45056, 49152, 53248, 57344, 61440, and 8192.	32768

Variable	Description	Default
vlan-range <vlan_map>	Enter the VLANs to which STP applies. <vlan_map> is a comma-separated list of VLAN IDs or VLAN ID ranges, for example “1,3-4,6,7,9-100” .	No default
config stp-port		
<port name>	Enter the name of the port.	No default
cost <cost_int>	Enter the cost of using this interface. Use `set cost ?` for suggested cost values based on link speed.	0
priority <priority_int>	Enter the priority of this interface. Use `set priority ?` to list the acceptable priority values.	128

Example

```
config switch stp instance
   edit "1"
      set priority 8192
      config stp-port
         edit "port18"
            set cost 0
            set priority 128
         next
         edit "port19"
            set cost 0
            set priority 128
         next
      end
      set vlan-range 5 7 11-20
   end
```

config switch stp settings

Use this command to configure STP settings.

Syntax

```
config switch stp settings
   set forward-time <fseconds_int>
   set hello-time <hseconds_int>
   set max-age <age>
   set max-hops <hops_int>
   set name <name_str>
   set revision <rev_int>
   set status {enable | disable}
end
```

Variable	Description	Default
forward-time <fseconds_int>	Enter the forwarding delay in seconds. Range 4 to 30.	15
hello-time <hseconds_int>	Enter the hello time in seconds. Range 1 to 10.	2
max-age <age>	Enter the maximum age. Range 6 to 40.	20
max-hops <hops_int>	Enter the maximum number of hops. Range 1 to 40.	20
name <name_str>	Enter a string value for the name.	No default
revision <rev_int>	Range 0 to 65535.	0
status {enable | disable}	Enable or disable status report.	enable

Example

```
config switch stp settings
   set forward-time 15
   set hello-time 5
   set max-age 20
   set max-hops 20
   set name "region1"
   set revision 1
   set status enable
end
```

config switch trunk

Use this command to configure link aggregation.

Syntax

```
config switch trunk
   edit <trunk name>
      set auto-isl <integer>
      set bundle [enable|disable]
         set min_bundle <integer>
         set max_bundle <integer>
      set description <description_str>
      set mclag {disable | enable}
      set mclag-icl {disable | enable}
      set members <intf1 ... intfn>
      set mode {fortinet-trunk | lacp-active | lacp-passive | static}
      set port-selection-criteria {src-ip | src-mac | dst-ip | dst-mac | src-dst-ip | src-
          dst-mac}
```

Variable	Description	Default
<trunk name>	Enter a name for the trunk.	No default

Variable	Description	Default
auto-isl <integer>	Automatically forms an ISL-encapsulated trunk, up to the specified maximum size.	0
bundle [enable|disable]	Enable or disable bundling	disable
min_bundle	Set the minimum size of the bundle. This option is available only when `bundle` has been enabled.	1
max_bundle	Set the maximum size of the bundle. This option is available only when `bundle` has been enabled.	24
description <description_str>	Optionally, enter a description.	No default
mclag {disable | enable}	Enable or disable multichassis LAG (MCLAG).	disable
mclag-icl {disable | enable}	Enable or disable the MCLAG inter-chassis link (ICL).	disable
members <intf1 … intfn>	Enter the names of the interfaces that belong to this trunk. Separate the names with spaces.	No default
mode {fortinet-trunk | lacp-active | lacp-passive | static}	Select the link aggregation mode: • `fortinet-trunk` — use heartbeat packets to detect whether trunk members are available. • `lacp-active` — use active LACP 802.3ad aggregation • `lacp-passive` — use passive LACP 802.3ad aggregation • `static` — use static aggregation, ignoring and not sending control messages	static
port-selection-criteria {src-ip | src-mac | dst-ip | dst-mac | src-dst-ip | src-dst-mac}	Select the port selection criteria: • `src-ip` — source IP address • `src-mac` — source MAC address • `dst-ip` — destination IP address • `dst-mac` — destination MAC address • `src-dst-ip` — both source and destination IP addresses • `src-dst-mac` — both source and destination MAC addresses	src-dst-ip

Heartbeat Trunk

When you set the trunk mode to fortinet-trunk, the following configuration fields are available:

```
config switch trunk
   edit hb-trunk
      set mode fortinet-trunk
      set port-selection-criteria {src-ip | src-mac | dst-ip | dst-mac | src-dst-ip | src-
          dst-mac}
```

```
        set description <description_str>
        set members <port> [<port>] ... [<port>]
        set member-withdrawal-behavior {block | forward}
        set max-miss-heartbeats <3-32>
        set hb-out-vlan <int>
        set hb-in-vlan <int>
        set hb-src-ip <x.x.x.x>
        set hb-dst-ip <x.x.x.x>
        set hb-src-udp-port <int>
        set hb-dst-udp-port <int>
        set hb-verify {enable | disable}
    end
```

Variable	Description	Default
port-selection-criteria {src-ip | src-mac | dst-ip | dst-mac | src-dst-ip | src-dst-mac}	Select the port selection criteria: • `src-ip` — source IP address • `src-mac` — source MAC address • `dst-ip` — destination IP address • `dst-mac` — destination MAC address • `src-dst-ip` — both source and destination IP addresses • `src-dst-mac` — both source and destination MAC addresses	src-dst-ip
description <description_str>	Optionally, enter a description.	No default
members <port> [<port>] ... [<port>]	Enter the names of the ports that belong to this trunk. Separate the names with spaces.	No default
member-withdrawal-behavior {block | forward}	Set the port behavior after it withdraws because of the loss of control packets.	block
max-miss-heartbeats <3-32>	Enter the maximum number of heartbeat messages that can be lost before the FortiGate is deemed to be unavailable. Set a value between 3 and 32.	10
hb-out-vlan	Enter the outgoing VLAN value.	0
hb-in-vlan	Enter the incoming VLAN value.	0
hb-src-ip	Enter the source IP address for the heartbeat packet.	0.0.0.0
hb-dst-ip	Enter the destination IP address for the heartbeat packet.	0.0.0.0
hb-src-udp-port	Enter the source UDP port value for the heartbeat packet.	0
hb-dst-udp-port	Enter the destination UDP port value for the heartbeat packet.	0
hb-verify	Enable or disable heartbeat packet verification.	disable

Example

The following example creates trunk tr1 with heartbeat capability:

```
config switch trunk
   edit "tr1"
      set mode fortinet-trunk
      set members "port1" "port2"
      set hb-out-vlan 300
      set hb-in-vlan 500
      set hb-src-ip 10.105.7.200
      set hb-dst-ip 10.105.7.199
      set hb-src-udp-port 12345
      set hb-dst-udp-port 54321
      set hb-verify enable
   next
end
```

config switch virtual-wire

Use this command to forward traffic between two ports with minimal filtering or packet modifications. The VLAN setting is optional.

NOTE: Virtual-wire ports will not be able to transmit or receive packets from other members of the VLAN or other virtual-wires that use the same VLAN. The VLAN should not have complex configurations such as private VLAN.

Syntax

```
config switch virtual-wire
   edit <id>
      set first-member <port>
      set second-member <port>
      set vlan <1-4095>
```

Variable	Description	Default
<id>	Enter a unique integer to create a new entry.	No default
first-member <port>	first member in the virtual-wire pair	No default
second-member <port>	second member in the virtual-wire pair	No default
vlan <1-4095>	VLAN used. The VLAN can be shared between virtual-wires and non-virtual-wire ports	4011

Example

The following example creates a virtual wire between ports 7 and 8:

```
config switch virtual-wire
   edit 1
      set first-member "port7"
      set second-member "port8"
      set vlan 70
   end
```

config switch vlan

Use this command to configure VLANs.

Syntax

```
config switch vlan
   edit <vlan id>
      set description <description_str>
      set learning-limit <integer>
      set dhcp-snooping {enable | disable}
         set dhcp-snooping-verify-mac {enable | disable}
         set dhcp-snooping-option82 {enable | disable}
         set arp-inspection {enable | disable}
      set igmp-snooping {enable | disable}
         set igmp-snooping-querier {enable | disable}
            set querier-addr <IPv4_address>
      set private-vlan {enable | disable}
         set isolated-vlan <integer>
         set community-vlans <vlan_map>
```

Variable	Description	Default
<vlan id>	Enter a VLAN identifier.	No default
description <description_str>	Optionally, enter a description.	No default
learning-limit <integer>	Limit the number of dynamic MAC addresses on this VLAN. The per-VLAN MAC address learning limit is between 1 and 128. Set the value to 0 for no limit.	0
dhcp-snooping	Enable or disable DHCP snooping for this VLAN.	disable
dhcp-snooping-verify-mac	Enable or disable whether to verify the source MAC address. This field is available only if `dhcp-snooping` is enabled.	disable
dhcp-snooping-option82	Enable or disable whether to insert option-82 fields. This field is available only if `dhcp-snooping` is enabled.	disable
arp-inspection {enable | disable}	Enable or disable dynamic ARP inspection.	disable
igmp-snooping {enable | disable}	Enable or disable IGMP snooping on the VLAN.	disable
igmp-snooping-querier {enable | disable}	Enable or disable whether periodic IGMP queries are sent to get IGMP reports. This field is only available if `igmp-snooping` is enabled.	disable

Variable	Description	Default
querier-addr <IPv4_address>	Enter the IPv4 address for the IGMP querier. This field if only available if `igmp-snooping` and `igmp-snooping-querier` are enabled.	0.0.0.0
private-vlan	Set to enable if this is a private VLAN.	disable
isolated-vlan	(Valid if private VLAN is enabled) Enter the isolated VLAN.	0
community-vlans	(Valid if private VLAN is enabled) Enter the communities within this private VLAN. Enter single VLANs or ranges of VLANS separated by commas without white space. For example: 1,3-4,6,7,9-100	No default

config member-by

Use this command to assign VLANs based on specific fields in the packet (source MAC address, source IP address, or layer-2 protocol).

```
config switch vlan
   edit <vlan id>
      config member-by-mac
         edit <id>
            set mac XX:XX:XX:XX:XX:XX
            set description <128 byte string>
         next
      end
      config member-by-ipv4
         edit <id>
            set address a.b.c.d/e
            set description <128-byte string>
         next
      end
      config member-by-ipv6
         edit <id>
            set prefix xx:xx:xx:xx::/prefix
            set description <128-byte string>
         next
      end
      config member-by-proto
         edit <id>
            set frametypes {ethernet2 | 802.3d | llc}
            set protocol <6-digit hex value>
      end
```

Variable	Description	Default
config member-by-mac		
edit <id>	For a new entry, enter an unused ID.	No default

Variable	Description	Default
mac XX:XX:XX:XX:XX:XX	Enter a MAC address. If the source MAC address of an incoming packet matches this value, the associated VLAN will be assigned to the packet.	00:00:00:00:00:00
description	Enter up to 128 characters	No default
config member-by-ipv4		
edit <id>	For a new entry, enter an unused ID.	No default
address a.b.c.d/e	Enter an IPv4 address and network mask. If the source IP address of an incoming packet matches this value, the associated VLAN will be assigned to the packet. The subnet mask must be a value in the range of 1-32.	0.0.0.0 0.0.0.0
description	Enter up to 128 characters	No default
config member-by-ipv6		
edit <id>	For a new entry, enter an unused ID.	No default
prefix xx:xx:xx:xx::/prefix	Enter an IPv6 prefix. If the source IP address of an incoming packet matches this value, the associated VLAN will be assigned to the packet. The /prefix must in the range of 1-64.	::/0
description	Enter up to 128 characters	No default
config member-by-proto		
edit <id>	For a new entry, enter an unused ID.	No default
frametypes {ethernet2 | 802.3d | llc}	Enter one or more Ethernet frame type. Set this value to `llc` for logical link control. Set this value to `802.3d` for 802.3d and SNAP.	ethernet2 802.3d llc
protocol <6-digit hex value>	Enter an Ethernet protocol value If the frametype and Ethernet protocol value of an incoming packet matches these values, the associated VLAN will be assigned to the packet. The value range is 0-65535.	0x0000

Example

The following example configures a VLAN:

```
config switch vlan
   edit 100
      config member-by-mac
         edit 1
            set description "pc2"
            set mac 00:21:cc:d2:76:72
```

```
        next
      end
   end
end
```

The following example configures the IGMP querier:

```
config switch vlan
   edit 100
      set igmp-snooping enable
      set igmp-snooping-querier enable
      set querier-addr 1.2.3.4
   next
end
```

config system

Use the `config system` commands to configure options related to the overall operation of the FortiSwitch:

config system accprofile

Use this command to add access profile groups that control administrator access to FortiSwitch features. Each FortiSwitch administrator account must include an access profile. You can create access profiles that deny access, allow read only, or allow both read and write access to FortiSwitch features.

Syntax

```
config system accprofile
   edit <profile-name>
      set admingrp {none | read | read-write}
      set loggrp {none | read | read-write}
      set netgrp {none | read | read-write}
      set routegrp {none | read | read-write}
      set sysgrp {none | read | read-write}
   end
```

Variable	Description	Default
<profile-name>	Enter the name for the profile.	No default
admingrp {none | read | read-write}	Set the access permission for admingrp.	none
loggrp {none | read | read-write}	Set the access permission for loggrp.	none
netgrp {none | read | read-write}	Set the access permission for netgrp.	none
routegrp {none | read | read-write}	Set the access permission for routegrp.	none
sysgrp {none | read | read-write}	Set the access permission for sysgrp.	none

Example

This example shows how to configure an access profile with just read-only permission:

```
config system accprofile
   edit profile1
      set admingrp read
      set loggrp read
      set netgrp read
      set routegrp read
      set sysgrp read
   end
```

config system admin

Use the default admin account or an account with system configuration read and write privileges to add new administrator accounts and control their permission levels. Each administrator account except the default admin must include an access profile. You cannot delete the default super admin account or change the access profile (super_admin). In addition, there is also an access profile that allows read-only super admin privileges, super_admin_readonly. The super_admin_readonly profile cannot be deleted or changed, similar to the super_admin profile. This read-only super-admin may be used in a situation where it is necessary to troubleshoot a customer configuration without making changes.

You can authenticate administrators using a password stored on the FortiSwitch or you can use a RADIUS server to perform authentication. When you use RADIUS authentication, you can authenticate specific administrators or you can allow any account on the RADIUS server to access the FortiSwitch as an administrator.

Syntax

```
config system admin
   edit <admin_name>
      set accprofile <profile-name>
      set allow-remove-admin-session {enable | disable}
      set comments <comments_string>
      set gui-detail-panel-location {bottom | ide | side}
      set {ip6-trusthost1 | ip6-trusthost2 | ip6-trusthost3 |
      ip6-trusthost4 | ip6-tru sthost5 | ip6-trusthost6 |
      ip6-trusthost7 | ip6-trusthost8 | ip6-trusthost9 |
      ip6-trusthost10} <address_ipv6mask>
      set password <admin_password>
      set peer-auth {disable | enable}
         set peer-group <peer-grp>
      set remote-auth {enable | disable}
         set remote-group <name>
         set wildcard {enable | disable}
      set schedule <schedule-name>
      set ssh-public-key1 "<key-type> <key-value>"
      set ssh-public-key2 "<key-type> <key-value>"
      set ssh-public-key3 "<key-type> <key-value>"
      set {trusthost1 | trusthost2 | trusthost3 | trusthost4 |
      trusthost5 | trusthost6 | trusthost7 | trusthost8 | trusthost9
      | trusthost10} <address_ipv4mask>
      end
   end
```

Variable	Description	Default
<admin_name>	Enter the name for the admin account.	No default
accprofile <profile-name>	Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiSwitch features.	No default
allow-remove-admin-session {enable | disable}	Allow admin session to be removed by privileged admin users	disable
comments <comments_string>	Enter the last name, first name, email address, phone number, mobile phone number, and pager number for this administrator. Separate each attribute with a comma, and enclose the string in double-quotes. The total length of the string can be up to 128 characters. (Optional)	No default
gui-detail-panel-location {bottom | hide | side}	Choose the position of the log detail window.	bottom

Variable	Description	Default
{ip6-trusthost1 | ip6-trusthost2 | ip6-trusthost3 | ip6-trusthost4 | ip6-trusthost5 | ip6-trusthost6 | ip6-trusthost7 | ip6-trusthost8 | ip6-trusthost9 | ip6-trusthost10} <address_ipv6mask>	Any IPv6 address and netmask from which the administrator can connect to the FortiSwitch. If you want the administrator to be able to access the system from any address, set the trusted hosts to ::/0.	::/0
password <admin_password>	Enter the password for this administrator. It can be up to 256 characters in length.	No default
peer-auth {disable | enable}	Set to enable peer certificate authentication (for HTTPS admin access).	disable
peer-group <peer-grp>	Name of peer group defined under `config user peergrp` or user group defined under `config user group`. Used for peer certificate authentication (for HTTPS admin access). This option is available only when `peer-auth` has been enabled.	No default
remote-auth {enable | disable}	Enable or disable authentication of this administrator using a remote RADIUS, LDAP, or TACACS+ server.	disable
remote-group <name>	Enter the administrator user group name, if you are using RADIUS, LDAP, or TACACS+ authentication. This is available only when `remote-auth` is enabled.	No default
wildcard {enable | disable}	Enable or disable wildcard RADIUS authentication. This option is available only when `remote-auth` is enabled.	disable
schedule <schedule-name>	Restrict times that an administrator can log in. Defined in `config firewall schedule`. No default indicates that the administrator can log in at any time.	No default
ssh-public-key1 "<key-type> <key-value>"	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. `<key type>` is `ssh-dss` for a DSA key or `ssh-rsa` for an RSA key. `<key-value>` is the public key string of the SSH client.	No default
ssh-public-key2 "<key-type> <key-value>"		No default
ssh-public-key3 "<key-type> <key-value>"		No default

Variable	Description	Default
{trusthost1 | trusthost2 | trusthost3 | trusthost4 | trusthost5 | trusthost6 | trusthost7 | trusthost8 | trusthost9 | trusthost10} <address_ipv4mask>	Any IPv4 address or subnet address and netmask from which the administrator can connect to the system. If you want the administrator to be able to access the system from any address, set the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0.	0.0.0.0 0.0.0.0

Example

The following example creates a RADIUS system admin group:

```
config system admin
   edit "RADIUS_Admins"
      set remote-auth enable
      set accprofile "super_admin"
      set wildcard enable
      set remote-group "RADIUS_Admins"
   next
end
```

config system arp-table

Use this command to manually add ARP table entries to the FortiSwitch. ARP table entries consist of a interface name, an IP address, and a MAC address.

Syntax

```
config system arp-table
   edit <table_value>
      set interface {<string> | internal | mgmt}
      set ip <address_ipv4>
      set mac <mac_address>
   end
```

Variable	Description	Default
<table_value>	Enter the identification number for the table.	No default
interface {<string> | internal | mgmt}	Enter the interface to associate with this ARP entry	No default
ip <address_ipv4>	Enter the IP address of the ARP entry.	0.0.0.0
mac <mac_address>	Enter the MAC address of the device entered in the table, in the form of xx:xx:xx:xx:xx:xx.	00:00:00:00:00:00

Example

This example shows how to add an entry to an ARP table:

```
config system arp-table
   edit 1
```

```
    set interface internal
    set ip 172.168.20.1
    set mac 00:21:cc:d2:76:72
  end
```

config system bug-report

Use this command to configure a custom email relay for sending problem reports to Fortinet customer support.

Syntax

```
config system bug-report
  set auth {no | yes}
  set mailto <email_address>
  set password <password>
  set server <servername>
  set username <name>
  set username-smtp <account_name>
end
```

Variable	Description	Default
auth {no | yes}	Enter `yes` if the SMTP server requires authentication or `no` if it does not.	no
mailto <email_address>	The email address for bug reports.	fortiswitch@fortinet.com
password <password>	If the SMTP server requires authentication, enter the required password.	No default
server <servername>	The SMTP server to use for sending bug report email.	fortinet.com
username <name>	A valid user name on the specified SMTP server.	bug_report
username-smtp <account_name>	A valid user name for authentication on the specified SMTP server.	bug_report

Example

This example shows how to configure a custom email relay:

```
config system bug-report
  set auth yes
  set mailto techdocs@fortinet.com
  set password 123abc
  set server fortinet.com
  set username techdocs
  set username-smtp techdocs
  end
```

config system certificate ca

Use this command to configure CA certificates.

FortiSwitch includes a reserved entry named `Fortinet_CA`. You cannot modify this entry.

Syntax

```
config system certificate ca
   edit <name>
      set ca <certificate>
      set scep-url <string>
   next
end
```

Variable	Description	Default
name	Enter the name of the certificate.	No default
certificate	PEM format CA certificate. Paste the contents of a CA certificate file between quotation marks as shown in the example.	No default
set scep-url	Full URL (such as http://www.test.com)	No default

Example

```
# config system certificate ca
# get
== [ Fortinet_CA ]
== [ OracleSSLCA ]
== [ ca ]
FortiCore-VM # config system certificate ca
FortiCore-VM (ca) # edit ca-new
FortiCore-VM (ca-new) # set certificate "-----BEGIN CERTIFICATE-----
> MIID0TCCArmgAwIBAgIJAKr1/WtE48FeMA0GCSqGSIb3DQEBCwUAMGgxEzARBgoJ
> kiaJk/IsZAEZFgNvcmcxFzAVBgoJkiaJk/IsZAEZFgdjaWxvZ29uMQswCQYDVQQG
> EwJVUzEQMA4GA1UEChMHQ0lMb2dvbjEZMBcGA1UEAxMQQ0lMb2dvbiBPU0cgQ0Eg
> MTAeFw0xNDA0MzAxNDE4MDhaFw0zNDA0MzAxNDE4MDhaMGgxEzARBgoJkiaJk/Is
> ZAEZFgNvcmcxFzAVBgoJkiaJk/IsZAEZFgdjaWxvZ29uMQswCQYDVQQGEwJVUzEQ
> MA4GA1UEChMHQ0lMb2dvbjEZMBcGA1UEAxMQQ0lMb2dvbiBPU0cgQ0EgMTCCASIw
> DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMQQzsB9Uc37VuIyt5xJxcYYkc6K
> XpYihHgskTQp6YYB4XHVimouHafMYyoFsnenrcgf2NGFDvi9l9x9mnL77920JqGr
> LijieMiFEyP1nhGW8C6nJjkSsXLbgZNh9u6U+0oAbspsFRwdHDZOI7gIHSJ2zuiY
> CkMAvjw9TN44Q4IFCvSIf7mfzZgBH7AW1sbgznqnAJsWQhQGTpxZAxubItesyduD
> vj8tz9eb5u8JO3iQ/LYhMspNnxcpTFdaLn2v82NAFTtCrZdCd7aLj1DM0DPEX7Nw
> V/rt/l+tlscglYyEoUnlPYuSQN0Q6Aj5i1GcKPvnFS0Oy9lGY1lT1vZJ4F0CAwEA
> AaN+MHwwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYE
> FP7bnvI4TIqtrM+KGgCvedJiQpuHMB8GA1UdIwQYMBaAFP7bnvI4TIqtrM+KGgCv
> FP7bnvI4TIqtrM+KGgCvedJiQpuHMBkGA1UdEQQSMBCBDmNhQGNpbG9nb24ub3JnMA0GCSqGSIb3DQEBCwUA
> A4IBAQCq5KUHQNg51uh1pxKMXQ98ADj2bNzQbswdAFslPow8tTZIBMwhdrq02ZHC
> XPyp2IHxfv+G+pMV1JFtdR0fy8ivilMNyjObEGh1Ss3kvvU7d1z3XwPxqpNcwDqs
> 1K6RRg4zpNWCFPcliAkPDsDbaN1B6A6zJXqOpGgzwocU3dZbPe5sYLgkWZO2/8MI
> eAEk7zoU1ZPSZiu5HghPafKuE1HYshvsak090tRgC6VLvaSLoNZlwR0GuFVGdewH
> 4jR1HpENH7QiLCB1NGCoJgDi3qiFosw3M2+0ExevE1afj2Usm4oZir+Uty0rvR8D
```

```
> 03RHH8yYbZ9rw0kuwTkJEo3bYDxH
> -----END CERTIFICATE-----"
```

config system certificate crl

Use this command to configure the certificate revocation list.

Syntax

```
config system certificate crl
edit <name>
   set crl <crl>
   set http-url <string>
   set ldap-server <LDAP>
   set scep-cert <certificate>
   set scep-url <string>
end
```

Variable	Description	Default
name	Name of the certificate revocation list	No default
crl	PEM format CRL. Paste the contents of a CRL file between quotation marks.	No default
http-url	URL of HTTP server for CRL update	No default
ldap-server	LDAP server	No default
scep-cert	Local certificate used for CRL update using SCEP	Fortinet_ Factory
scep-url	URL of CA server for CRL update using SCEP	No default

config system certificate local

Use this command to manage local certificates. FortiSwitch includes a reserved entry named “Factory”. You cannot modify this entry.

Syntax

```
config system certificate local
   edit <name>
      set comments <string>
      set password <passwd>
      set private-key <key>
      set scep-url <string>
   next
end
```

Variable	Description	Default
name	Enter the name of the certificate.	No default
comments	Optional administrator note.	No default
password	Password that was used to encrypt the file. The FortiCore system uses the password to decrypt and install the certificate.	*
private-key	Paste the contents of a key file between quotation marks as shown in the example.	No default
scep-url	URL of SCEP server	No default

Example

```
 # config system certificate local
 # get
       == [ Factory ]
       == [ csr_name_test ]
# show
config system certificate local
edit "csr_name_test"
t7e4fiX6Sd6T5426Gg/HQXRH41mBwGmjKdBSHUbVUZTka2FtD1oLMWE2mTq1c9GMUz0DokP-
foqxkjkmja5mWv4/w
A5XdQ00lQmTeMZK/X5OSFmSS
set private-key "-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBnjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5/vf1VQB/28CAggA
MBQGCCqGSIb3DQMHBAgZorM0zlnPNASCAViZk4wTZYYMPl0e7NwyxqvLND3LxUaV
UG1XpUSPfnUP4YgrV2d0Uijclj5M7MS341cMVKZ7G1pS/6jvxUr0NamQv4j7JsJ0
t3G7LMkzcTiep26GUCy55Qt+iob7lh0iiKa+4uPOq/Mzy+84AWnRNLfIhevHPsYb
rk4UbwNOFb0ZD9i06+UrFLsRGmtp/vlDyBgAoBojKxB/4j0G299QamnzPz4qneBc
HtPqTMPELyqtT6w4cmnwp6Ti2OOAr9c44mKdyyAVZKie+Iu/4pSVBNSfuC+jjtmC
k8OrCrG14NwrhbTY9zEnGxBRR1NMTEBBTqAQNYWtjUEQVjmY1GAJA3/oBQe7l8C/
G/IUVvc/aaqMvsKSNfDpgZaudTDe1Wxi1792ADGh7zslls+ykH9nmqh7BPfm30Nv
f8O1hXgq01Lvo4v1xdC0w5oAeCyGlbTY5ZnXJFm0HCp0kA==
-----END ENCRYPTED PRIVATE KEY-----
"
set csr "-----BEGIN CERTIFICATE REQUEST-----
MIIBNzCB4gIBADBqMQswCQYDVQQIEwJjYTESMBAGA1UEBxMJc3Vubnl2YWxlMREw
DwYDVQQKEwhmb3J0aW5ldDENMAsGA1UECxMEZmFkYzEQMA4GA1UEAxMHZXhhbXBs
ZTETMBEGCSqGSIb3DQEJARYEcm9vdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDK
XH/MC1KTkkZJiQDFb6IXHLYsSVbJzF0K30s3CVmKZvJQSBnmV8aq3fJjN281rrFT
iUovVdBzwCF5jKbxsrPLAgMBAAGgEzARBgNVHRMxChMIQ0E6RkFMU0UwDQYJKoZI
hvcNAQEFBQADQQB96NU+xjds83/6VRSzsyxeVxAGVD7F9Npuji8r/MpxPiMT0PQM
G8Wg//26ZqpwjuPq2V1+7QU4MDk3B5VUJSEF
-----END CERTIFICATE REQUEST-----
"
```

config system certificate ocsp

Use this command to configure the OCSP server certificate.

Syntax

```
config system certificate ocsp
   set cert {<string> | Entrust_802.1x_CA | Entrust_802.1x_G2_CA | Entrust_802.1x_L1K_CA |
       Fortinet_CA | Fortinet_CA2}
   set unavail-action {ignore | revoke}
   set url <string>
end
```

Variable	Description	Default
cert {<string> | Entrust_802.1x_CA | Entrust_802.1x_G2_CA | Entrust_802.1x_L1K_CA | Fortinet_CA | Fortinet_CA2}	Enter the name of the certificate or select one of the listed certificates.	No default
unavail-action {ignore | revoke}	Set if the FortiSwitch should ignore the OCSP check or revoke the certificate if the server is unavailable.	revoke
url <string>	Enter the URL for the OCSP server.	No default

Example

This example shows how to configure the OCSP server certificate:

```
config system certificate ocsp
   set cert Fortinet_CA
   set unavail-action ignore
   set url https://www.fortinet.com
end
```

config system certificate remote

Use this command to install remote certificates. The remote certificates are public certificates without a private key.

```
config system certificate remote
   edit <name>
      set remote "<cert>"
   end
```

Variable	Description	Default
name	Name for the certificate	No default
remote "<cert>"	PEM-format certificate	No default

config system console

Use this command to set the console command mode, the number of lines displayed by the console, and the baud rate.

Syntax

```
config system console
   set baudrate <speed>
   set mode {batch | line}
   set output {standard | more}
end
```

Variable	Description	Default
baudrate <speed>	Set the console port baudrate. Select one of 9600, 19200, 38400, 57600, or 115200.	115200
mode {batch | line}	Set the console mode to line or batch. Used for autotesting only.	line
output {standard | more}	Set console output to standard (no pause) or more (pause after each screen is full and resume when a key is pressed). This setting applies to `show` or `get` commands only.	more

Example

This example shows how to configure the console:

```
config system console
   set baudrate 57600
   set mode batch
   set output standard
end
```

config system dns

Use this command to set the DNS server addresses. Several FortiSwitch functions, including sending email alerts and URL blocking, use DNS.

Syntax

```
config system dns
   set cache-notfound-responses {enable | disable}
   set dns-cache-limit <integer>
   set dns-cache-ttl <int>
   set domain <domain_name>
   set ip6-primary <dns_ipv6>
   set ip6-secondary <dns_ip6>
   set primary <dns_ipv4>
   set secondary <dns_ip4>
```

```
   set source-ip <ipv4_addr>
end
```

Variable	Description	Default
cache-notfound-responses {enable | disable}	Enable to cache NOTFOUND responses from the DNS server.	disable
dns-cache-limit <integer>	Set maximum number of entries in the DNS cache.	5000
dns-cache-ttl <int>	Enter the duration, in seconds, that the DNS cache retains information.	1800
domain <domain_name>	Set the local domain name (optional).	No default
ip6-primary <dns_ipv6>	Enter the primary IPv6 DNS server IP address.	::
ip6-secondary <dns_ip6>	Enter the secondary IPv6 DNS server IP address.	::
primary <dns_ipv4>	Enter the primary DNS server IP address.	0.0.0.0
secondary <dns_ip4>	Enter the secondary DNS IP server address.	0.0.0.0
source-ip <ipv4_addr>	Enter the IP address for communications to DNS server.	0.0.0.0

Example

This example shows how to set the DNS server addresses:

```
config system dns
   set cache-notfound-responses enable
   set dns-cache-limit 2000
   set dns-cache-ttl 900
   set domain fortinet.com
   set primary 172.91.112.53
   set secondary 172.91.112.52
end
```

config system fsw-cloud

Use this command to configure the FortiSwitch cloud manager. The FortiSwitch cloud manager allows you to quickly check the status and configuration of multiple FortiSwitches through a single management portal.

NOTE: To use the FortiSwitch cloud manager, your FortiSwitch must be connected to the Internet, and the system time must be accurate. To set your the time on your FortiSwitch, see config system ntp on page 109.

Syntax

```
config system fsw-cloud
   set interval <integer>
   set name <string>
   set port <port_number>
   set status {enable | disable}
end
```

Variable	Description	Default
interval <integer>	The time in seconds allowed for domain name system (DNS) resolution. The value range is 3-300 seconds.	15
name <string>	The domain name for the FortiSwitch cloud manager.	fortiswitch-dispatch.forticloud.com
port <port_number>	Port number used to connect to the FortiSwitch cloud manager.	443
status {enable | disable}	Whether the FortiSwitch cloud manager is enabled or disabled.	disable

Example

This example shows how to configure the FortiSwitch cloud manager:

```
config system fsw-cloud
   set interval 150
   set name fortiswitch-dispatch.forticloud.com
   set port 443
   set status enable
end
```

config system global

Use this command to configure global settings that affect various FortiSwitch systems and configurations.

Syntax

```
config system global
   set 802.1x-ca-certificate {Entrust_802.1x_CA | Entrust_802.1x_G2_CA | Entrust_802.1x_
       L1K_CA | Fortinet_CA}
   set 802.1x-certificate {Entrust_802.1x | Fortinet_Factory | Fortinet_Firmware}
   set admin-concurrent {enable | disable}
   set admin-https-pki-required {enable | disable}
   set admin-https-ssl-versions {tlsv1-0 | tlsv1-1 | tlsv1-2}
   set admin-lockout-duration <time_int>
   set admin-lockout-threshold <failed_int>
   set admin-port <port_number>
   set admin-scp {enable | disable}
   set admin-server-cert {self-sign | Entrust_802.1x | Fortinet_Factory | Fortinet_
       Firmware}
   set admin-sport <port_number>
   set admin-ssh-grace-time <time_int>
   set admin-ssh-port <port_number>
   set admin-ssh-v1 {enable | disable}
   set admin-telnet-port <port_number>
   set admintimeout <admin_timeout_minutes>
   set allow-subnet-overlap {enable | disable}
   set asset-tag <string>
   set cfg-save {automatic | manual | revert}
```

```
    set csr-ca-attribute {enable | disable}
    set daily-restart {enable | disable}
    set detect_ip_conflict {enable | disable}
    set dst {enable | disable}
    set gui-lines-per-page <gui_lines>
    set hostname <unithostname>
    set image-rotation {enable | disable}
    set kernel-crashlog {enable | disable}
    set language <language>
    set ldapconntimeout <ldaptimeout_msec>
    set radius-port <radius_port>
    set refresh <refresh_seconds>
    set remoteauthtimeout <timeout_sec>
    set revision-backup-on-logout {enable | disable}
    set revision-backup-on-upgrade {enable | disable}
    set strong-crypto {enable | disable}
    set switch-mgmt-mode {fortilink | local}
    set timezone <timezone_number>
    set user-server-cert {self-sign | Entrust_802.1x | Fortinet_Factory | Fortinet_
        Firmware}
end
```

Variable	Description	Default
802.1x-ca-certificate {Entrust_802.1x_CA | Entrust_802.1x_G2_CA | Entrust_802.1x_L1K_CA | Fortinet_CA}	Set the CA certificate for port security (802.1x).	Entrust_802.1x_CA
802.1x-certificate {Entrust_802.1x | Fortinet_Factory | Fortinet_Firmware}	Set the certificate for port security (802.1x).	Entrust_802.1x
admin-concurrent {enable | disable}	Enable to enforce concurrent administrator logins. When enabled, the FortiSwitch restricts concurrent access from the same admin user name but on different IP addresses. Use `policy-auth-concurrent` for firewall authenticated users.	enable
admin-https-pki-required {enable | disable}	Enable to allow user to login by providing a valid certificate if PKI is enabled for HTTPS administrative access. The default setting of `disable` allows admin users to log in by providing a valid certificate or password.	disable
admin-https-ssl-versions {tlsv1-0 | tlsv1-1 | tlsv1-2}	Set the allowed SSL/TLS versions for Web administration.	tlsv1-1 tlsv1-2
admin-lockout-duration <time_int>	Set the administration account's lockout duration in seconds for the firewall. Repeated failed login attempts will enable the lockout. Use admin-lockout-threshold to set the number of failed attempts that will trigger the lockout.	60

Variable	Description	Default
admin-lockout-threshold <failed_int>	Set the threshold, or number of failed attempts, before the account is locked out for the admin-lockout-duration.	3
admin-port <port_number>	Enter the port to use for HTTP administrative access.	80
admin-scp {enable | disable}	Enable to allow system configuration download by the secure copy (SCP) protocol.	disable
admin-server-cert { self-sign | Entrust_802.1x | Fortinet_Factory | Fortinet_Firmware }	Select the admin https server certificate to use. Choices include self-sign, and the file name of any installed certificates.	Fortinet_Firmware
admin-sport <port_number>	Enter the port to use for HTTPS administrative access.	443
admin-ssh-grace-time <time_int>	Enter the maximum time permitted between making an SSH connection to the FortiSwitch and authenticating. Range is 10 to 3600 seconds.	120
admin-ssh-port <port_number>	Enter the port to use for SSH administrative access.	22
admin-ssh-v1 {enable | disable}	Enable compatibility with SSH v1.0.	disable
admin-telnet-port <port_number>	Enter the port to use for telnet administrative access.	23
admintimeout <admin_timeout_minutes>	Set the number of minutes before an idle administrator times out. This controls the amount of inactive time before the administrator must log in again. The maximum `admintimeout` interval is 480 minutes (8 hours). To improve security keep the idle timeout at the default value of 5 minutes.	5
allow-subnet-overlap {enable | disable}	Enable limited support for interface and VLAN subinterface IP address overlap for this VDOM. Use this command to enable limited support for overlapping IP addresses in an existing network configuration. **Caution: for advanced users only**. Use this only for existing network configurations that cannot be changed to eliminate IP address overlapping.	disable
asset-tag	LLDP uses the asset tag to help identify the unit. The asset tag can be up to 32 characters, and will be added to the LLDP-MED inventory TLV (when that TLV is enabled).	No default

Variable	Description	Default
cfg-save {automatic | manual | revert}	Set the method for saving the FortiSwitch system configuration and enter into runtime-only configuration mode. Methods for saving the configuration are: `automatic` automatically save the configuration after every change. `manual` manually save the configuration using the "execute" on page 201 command. `revert` manually save the current configuration and then revert to that saved configuration after `cfg-revert-timeout` expires. Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode.	automatic
csr-ca-attribute {enable | disable}	Enable to use the CA attribute in your certificate. Some CA servers reject CSRs that have the CA attribute.	enable
daily-restart {enable | disable}	Enable to restart the FortiSwitch every day. The time of the restart is controlled by `restart-time`.	disable
detect_ip_conflict	Enable the Detect IP Conflict feature.	enable
dst {enable | disable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiSwitch adjusts the system time when the time zone changes to daylight saving time and back to standard time.	enable
gui-lines-per-page <gui_lines>	Set the number of lines displayed on table lists. Range is from 20 - 1000 lines per page.	50
hostname <unithostname>	Enter a name to identify this FortiSwitch. A hostname can only include letters, numbers, hyphens, and underlines. No spaces are allowed. While the hostname can be longer than 16 characters, if it is longer than 16 characters it will be truncated and end with a “~” to indicate it has been truncated. This shortened hostname will be displayed in the CLI, and other locations the hostname is used. Some models support hostnames up to 35 characters. By default the hostname of your system is its serial number which includes the model.	FortiSwitch serial number.
image-rotation {enable | disable}	Enable or disable the rotation of the partition used to upgrade the FortiSwitch image.	disable
kernel-crashlog {enable | disable}	Enable or disable whether to log a kernel crash.	enable

Variable	Description	Default
language <language>	Set the display language. You can set `<language>` to one of `english`, `french`, `japanese`, `korean`, `portuguese`, `spanish`, `simch` (Simplified Chinese) or `trach` (Traditional Chinese).	english
ldapconntimeout <ldaptimeout_msec>	LDAP connection timeout in msec	500
radius-port <radius_port>	Change the default RADIUS port. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port on your system.	1812
refresh <refresh_seconds>	Set the Automatic Refresh Interval, in seconds, for the System Status Monitor. Enter 0 for no automatic refresh.	0
remoteauthtimeout <timeout_sec>	The number of seconds that the FortiSwitch waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. The range is 0 to 300 seconds, 0 means no timeout. To improve security keep the remote authentication timeout at the default value of 5 seconds. However, if a RADIUS request needs to traverse multiple hops or several RADIUS requests are made, the default timeout of 5 seconds may not be long enough to receive a response.	5
revision-backup-on-logout {disable | enable}	Enable or disable backing up the latest configuration revision when the administrator logs out of the CLI or Web GUI.	enable
revision-backup-on-upgrade {enable | disable}	Enable or disable backing up the latest configuration revision when the administrator starts an upgrade.	enable
strong-crypto {enable | disable}	Strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.	disable
switch-mgmt-mode {fortilink | local}	Determines whether the switch is being managed locally, or managed by a FortiGate via a Fortilink connection.	local
timezone <timezone_number>	The number corresponding to your time zone from 00 to 72. Press `?` to list time zones and their numbers. Choose the time zone for the FortiSwitch from the list and enter the correct number.	00

Variable	Description	Default
user-server-cert {self-sign | Entrust_802.1x | Fortinet_ Factory | Fortinet_Firmware}	Select the certificate to use for https user authentication.	Fortinet_ Factory

Example

This example shows how to set the lockout threshold to one attempt and the duration before the administrator can try again to log in to five minutes:

```
config system global
   set admin-lockout-threshold 1
   set admin-lockout-duration 300
end
```

config system interface

Use this command to edit the configuration of an interface.

If you enter a name string in the **edit** command that is not the name of a physical interface, the command creates a VLAN subinterface.

Syntax

```
config system interface
edit <interface_name>
   set allowaccess <access_types>
   set alias <name_string>
   set bfd {enable | disable | global}
      set bfd-desired-min-tx <interval_msec>
      set bfd-detect-mult <multiplier>
      set bfd-required-min-rx <interval_msec>
   set description <text>
   set dhcp-relay-service {enable | disable}
      set dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}
      set dhcp-relay-option82 {enable | disable}
   set external {enable | disable)
   set fail-detect {enable | disable}
      set fail-detect-option {link-down | detectserver}
      set fail-alert-method {link-d own | link-failed-signal}
      set fail-alert-interfaces {port1 port2 ...}
   set icmp-redirect {enable | disable}
   set ip <interface_ipv4mask>
   set log {enable | disable}
   set mode <static | dhcp>
      set dhcp-client-identifier <client_name_str>
      set defaultgw {enable | disable}
      set dns-server-override {enable | disable}
   set mtu-override {enable | disable}
   set secondary-IP {enable | disable}
   set snmp-index <integer>
   set status {down | up}
```

```
set type {loopback | vlan}
set vlanid <id_number>
set vrrp-virtual-mac {enable | disable}
```

A VLAN cannot have the same name as a zone or a virtual domain.

Variable	Description	Default
<interface_name>	Edit an existing interface or create a new VLAN interface.	No default
allowaccess <access_types>	Enter the types of management access permitted on this interface or secondary IP address. Valid types are: `http https ping radius-acct snmp ssh telnet`. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	Varies for each interface.
alias <name_string>	Enter an alias name for the interface. Once configured, the alias will be displayed with the interface name to make it easier to distinguish. The alias can be a maximum of 25 characters. This option is only available when interface type is `physical`.	No default.
bfd {enable | disable | global}	The status of bidirectional forwarding detection (bfd) on this interface: • `enable` — enable BFD and ignore global BFD configuration. • `disable` — disable BFD on this interface. • `global` — use the BFD configuration in `system settings` for the virtual domain to which this interface belongs.	global
bfd-desired-min-tx <interval_msec>	Enter the minimum desired interval for the BFD transmit interval. Valid range is from 1 to 100 000 msec. This option is available only when `bfd` is enabled.	50
bfd-detect-mult <multiplier>	Select the BFD detection multiplier. This option is available only when `bfd` is enabled.	3
bfd-required-min-rx <interval_msec>	Enter the minimum required interface for the BFD receive interval. Valid range is from 1 to 100 000 msec. This is available only when `bfd` is enabled.	50

Variable	Description	Default
description <text>	Optionally, enter up to 63 characters to describe this interface.	No default
dhcp-relay-service {enable | disable}	Enable to provide DHCP relay service on this interface. The DHCP type relayed depends on the setting of `dhcp-relay-type`. There must be no other DHCP server of the same type (regular or ipsec) configured on this interface.	disable
dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}	Set DHCP relay IP addresses. You can specify up to eight DHCP relay servers for DHCP coverage of subnets. Replies from all DHCP servers are forwarded back to the client. The client responds to the offer it wants to accept. Do not set `dhcp-relay-ip` to 0.0.0.0. This option is available only when `dhcp-relay-service` is enabled.	No default
dhcp-relay-option82 {enable | disable}	Enable to allow option-82 insertion in the DHCP relay. This option is available only when `dhcp-relay-service` is enabled.	disable
external {enable | disable)	Enable to indicate that an interface is an external interface connected to an external network. This option is used for SIP NAT when the `config VoIP profile` SIP `contact-fixup` option is disabled.	disable
fail-detect {enable | disable}	Enable interface failure detection.	disable
fail-detect-option {`link-down | detectserver`}	Select whether the system detects interface failure by port detection (`link-down`) or ping server (`detectserver`). This option is available only when `fail-detect` is enabled.	link-down
fail-alert-method {link-down | link-failed-signal}	Select the signal that the system uses to signal the link failure: Link Down or Link Failed. This option is available only when `fail-detect` is enabled.	link-down
fail-alert-interfaces {port1 port2 ...}	Select the interfaces to which failure detection applies. This option is available only when `fail-detect` is enabled.	No default
icmp-redirect {enable | disable}	Disable to stop ICMP redirect from sending from this interface. ICMP redirect messages are sent by a router to notify the original sender of packets that there is a better route available.	enable

Variable	Description	Default
ip <interface_ipv4mask>	Enter the interface IP address and netmask. This option is not available if `mode` is set to `dhcp`. You can set the IP and netmask, but they are not displayed. This is only available in NAT/Route mode. The IP address cannot be on the same subnet as any other interface.	Varies for each interface.
log {enable | disable}	Enable or disable traffic logging of connections to this interface. Traffic will be logged only when it is on an administrative port. All other traffic will not be logged. Enabling this setting may reduce system performance, and is normally used only for troubleshooting.	disable
mode <interface_mode>	Configure the connection mode for the interface as one of: `static` — configure a static IP address for the interface. `dhcp` — configure the interface to receive its IP address from an external DHCP server.	static
dhcp-client-identifier	Override the default DHCP client identifier used by this interface. The DHCP client identifier is used by DHCP to identify individual DHCP clients (in this case individual interfaces). By default, the DHCP client identifier for each interface is created based on the model name and the interface MAC address. In some cases, you might want to specify your own DHCP client identifier using this command. This option is available only when the `mode` is set to `dhcp`.	No default
defaultgw {enable | disable}	Enable to get the gateway IP address from the DHCP server. This option is available only when the `mode` is set to `dhcp`.	disable
dns-server-override {enable | disable}	Disable to prevent this interface from using DNS server addresses it acquires by DHCP. This option is available only when the `mode` is set to `dhcp`.	enable
mtu-override {enable | disable}	Select enable to use custom MTU size instead of default (1 500). This is available only for physical interfaces and some tunnel interfaces (not IPsec). If you change the MTU size, you must reboot the FortiSwitch to update the MTU values of the VLANs on this interface. Some models support MTU sizes larger than the standard 1 500 bytes.	disable
secondary-IP {enable | disable}	Enable to add a secondary IP address to the interface. This option must be enabled before configuring a secondary IP address. When disabled, the Web-based manager interface displays only the option to enable secondary IP.	disable
snmp-index <integer>	Configure the SNMP index	

Variable	Description	Default
status {down | up}	Start or stop the interface. If the interface is stopped, it does not accept or send packets. If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.	`up` (`down` for VLANs)
type {loopback | vlan}	Enter the type of interface. **NOTE:** Some types are read only, and are set automatically by hardware. • `loopback` — a virtual interface that is always up. This interface's status and link status are not affected by external changes. It is primarily used for blackhole routing - dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route. loopback interfaces have no dhcp settings, no forwarding, no mode, or dns settings. You can create a loopback interface from the CLI or Web-based manager. • `vlan` — a virtual LAN interface. This is the type of interface created by default on any existing physical interface. VLANs increase the number of network interfaces beyond the physical connections on the system. VLANs cannot be configured on a switch mode interface in Transparent mode.	vlan
vlanid <id_number>	Enter a VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. The VLAN ID can be any number between 1 and 4094, as 0 and 4095 are reserved, but it must match the VLAN ID added by the IEEE 802.1Q-compliant router on the other end of the connection. Two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN ID to different physical interfaces, and you can add more multiple VLANs with different VLAN IDs to the same physical interface. This is available only when editing an interface with a type of `VLAN`.	No default
vrrp-virtual-mac {enable | disable}	Enable VRRP virtual MAC addresses for the VRRP routers added to this interface. See RFC 3768 for information about the VRRP virtual MAC addresses.	disable

config ipv6

Configure IPv6 settings for the interface.

Syntax

```
config system interface
edit <interface_name>
```

```
config ipv6
   set ip6-address <if_ipv6mask>
   set ip6-allowaccess <access_types>
   config ip6-extra-address
      edit <prefix_ipv6>
   end
end
```

Variable	Description	Default
<interface_name>	Edit an existing interface or create a new VLAN interface.	No default
ip6-address <if_ipv6mask>	The interface IPv6 address and netmask. The format for IPv6 addresses and netmasks is described in RFC 3513. This is available in NAT/Route mode only.	::/0
ip6-allowaccess <access_types>	Enter the types of management access permitted on this IPv6 interface. Valid types are: `fgfm`, `http`, `https`, `ping`, `snmp`, `ssh`, and `telnet`. Separate the types with spaces. If you want to add or remove an option from the list, retype the list as required. >	Varies for each interface.
config ip6-extra-addr		
<prefix_ipv6>	IPv6 address prefix. Configure a secondary address for this IPv6 interface.	No default

config vrrp

Add one or more VRRP virtual routers to a interface. For information about VRRP, see RFC 3768.

Syntax

```
config system interface
edit <interface_name>
   config vrrp
      edit <VRID_int>
         set adv-interval <seconds_int>
         set preempt {enable | disable}
         set priority <prio_int>
         set start-time <seconds_int>
         set status {enable | disable}
         set vrdst <ipv4_addr>
         set vrgrp <integer>
         set vrip <ipv4_addr>
      end
```

Variable	Description	Default
<interface_name>	Edit an existing interface or create a new VLAN interface.	No default

Variable	Description	Default
<VRID_int>	VRRP virtual router ID (1 to 255). Identifies the VRRP virtual router.	None
adv-interval <seconds_int>	VRRP advertisement interval (1-255 seconds).	1
preempt {enable | disable}	Enable or disable VRRP preempt mode. In preempt mode a higher priority backup system can preempt a lower priority master system.	enable
priority <prio_int>	Priority of this virtual router (1-255). The VRRP virtual router on a network with the highest priority becomes the master.	100
start-time <seconds_int>	The startup time of this virtual router (1-255 seconds). The startup time is the maximum time that the backup system waits between receiving advertisement messages from the master system.	3
status {enable | disable}	Enable or disable this virtual router.	enable
vrdst <ipv4_addr>	Monitor the route to this destination.	0.0.0.0
vrgrp <integer>	VRRP group identifier. The value range is 1-65535.	0
vrip <ipv4_addr>	IP address of the virtual router.	0.0.0.0

Example

This example shows how to configure VRRP:

```
config system interface
   edit "vlan-8"
      set ip 10.10.10.1 255.255.255.0
      set allowaccess ping https http ssh
      set vrrp-virtual-mac enable
         config vrrp
            edit 5
               set priority 255
               set vrgrp 50
               set vrip 11.1.1.100
            next
            edit 6
               set priority 200
               set vrgrp 50
               set vrip 11.1.1.100
            next
            edit 7
               set priority 150
               set vrgrp 50
               set vrip 11.1.1.100
            next
         end
```

```
        set snmp-index 20
        set vlanid 8
        set interface "internal"
    next
end
```

config system link-monitor

Use this command to configure the link health monitor.

```
config system link-monitor
   edit <link monitor name>
      set srcintf <string>
      set protocol (arp | ping)
      set gateway-ip <IP address>
      set source-ip <IP address>
      set interval <integer>
      set timeout <integer>
      set failtime <integer>
      set recoverytime <integer>
      set update-cascade-interface (enable | disable)
      set update-static-route (enable | disable)
      set status (enable | disable)
   next
end
```

Variable	Description	Default
<link monitor name>	Enter the link monitor name.	No default
srcintf	Interface where the monitor traffic is sent.	No default
protocol	Protocols used to detect the server. Select ARP or ping.	arp
gateway-ip	Gateway IP used to PING the server.	0.0.0.0
source-ip	Source IP used in packet to the server.	0.0.0.0
interval	Detection interval in seconds. The range is 1-3600.	5
timeout	Detect request timeout in seconds. The range is 1-255.	1
failtime	Number of retry attempts before bringing server down. The range is 1-10.	5
recoverytime	Number of retry attempts before bringing server up. The range is 1-10.	5
update-cascade-interface	Enable or disable update cascade interface.	enable
update-static-route	Enable or disable update static route.	enable

Variable	Description	Default
status	Enable or disable link monitor administrative status.	enable

config system ntp

Use this command to configure Network Time Protocol (NTP) servers.

Syntax

```
config system ntp
   set allow-unsync-source {enable | disable}
   set ntpsync {enable | disable}
   set source-ip <ipv4_addr>
   set syncinterval <interval_int>
   config ntpserver
      edit <serverid_int>
         set ntpv3 {enable | disable}
         set server <ipv4_addr>[/<hostname_str>]
      end
   end
```

Variable	Description	Default
allow-unsync-source	Allow or do not allow an unsynchronized NTP source.	disable
ntpsync {enable | disable}	Enable to synchronize system time with the ntp server.	enable
source-ip <ipv4_addr>	Enter the source IP for communications to the NTP server.	0.0.0.0
syncinterval <interval_int>	Enter the interval in minutes between contacting NTP server to synchronize time. The range is from 1 to 1440 minutes. Only valid when `ntpsync` is enabled.	1
<serverid_int>	Enter the number for this NTP server	No default
ntpv3 {enable | disable}	Use NTPv3 protocol instead of NTPv4.	disable
server <ipv4_addr> [/<hostname_str>]	Enter the IPv4 address and hostname (optional) for this NTP server.	ntp1.fortinet.net

Example

This example shows how to configure an NTP server:

```
config system ntp
   set ntpsyn enable
   set syncinterval 5
   set source-ip 192.168.4.5
end
```

config system password-policy

Use this command to configure higher security requirements for administrator passwords and IPsec VPN pre-shared keys.

Syntax

```
config system password-policy
   set status {enable | disable}
      set apply-to [admin-password ipsec-preshared-key]
      set change-4-characters {enable | disable}
      set minimum-length <chars>
      set min-lower-case-letter <num_int>
      set min-upper-case-letter <num_int>
      set min-non-alphanumeric <num_int>
      set min-number <num_int>
      set expire-status {enable | disable}
         set expire-day <num_int>
end
```

Variable	Description	Default
status {enable | disable}	Enable password policy.	disable
apply-to [admin-password ipsec-preshared-key]	Select where the policy applies: administrator passwords or IPSec preshared keys. This option is available only when `status` is enabled.	admin-password
change-4-characters {enable | disable}	Enable to require the new password to differ from the old password by at least four characters. This option is available only when `status` is enabled.	disable
minimum-length <chars>	Set the minimum length of password in characters. Range 8 to 32. This option is available only when `status` is enabled.	8
min-lower-case-letter <num_int>	Enter the minimum number of required lower case letters in every password. This option is available only when `status` is enabled.	0
min-upper-case-letter <num_int>	Enter the minimum number of required upper case letters in every password. This option is available only when `status` is enabled.	0
min-non-alphanumeric <num_int>	Enter the minimum number of required non-alphanumeric characters in every password. This option is available only when `status` is enabled.	0
min-number <num_int>	Enter the minimum number of number characters required in every password. This option is available only when `status` is enabled.	0

Variable	Description	Default
expire-status {enable | disable}	Enable to have passwords expire. This option is available only when `status` is enabled.	enable
expire-day <num_int>	Enter the number of days before the current password is expired and the user will be required to change their password. This option is available only when `status` is enabled and `expire-status` is enabled.	90

Example

This example shows how to configure a password policy for administrator passwords:

```
config system password-policy
   set status enable
   set apply-to admin-password
   set change-4-characters enable
   set minimum-length 10
   set min-lower-case-letter 1
   set min-upper-case-letter 1
   set min-non-alphanumeric 1
   set min-number 1
   set expire-status enable
   set expire-day 30
end
```

config system settings

Use this comand to configure equal cost multi-path (ECMP) routing.

ECMP is a forwarding mechanism that enables load-sharing of traffic to multiple paths of equal cost. An ECMP set is formed when the routing table contains multiple next-hop address for the same destination with equal cost. Routes of equal cost have the same preference and metric value. If there is an ECMP set for an active route, the switch uses a hash algorithm to choose one of the next-hop addresses. As input to the hash, the switch uses one or more of the following fields in the packet to be routed:

- Source IP
- Destination IP
- Input port

Syntax

```
config system settings
   set v4-ecmp-mode {source-ip-based | dst-ip-based | port-based}
end
```

Variable	Description	Default
v4-ecmp-mode {source-ip-based | dst-ip-based | port-based}	Select the IPv4 ECMP mode: • `dst-ip-based` — Select the next hop based on the destination IP address. • `port-based` — Select the next hop based on the TCP/UDP port. • `source-ip-based` — Select the next hop based on the source IP address.	source-ip-based

Example

This example shows how to configure ECMP:

```
config system settings
   set v4-ecmp-mode port-based
end
```

config system sflow

Use this command to add or change the IP address and UDP port that FortiSwitch sFlow agents use to send sFlow datagrams to an sFlow collector.

sFlow is a network monitoring protocol described in http://www.sflow.org. FortiSwitch implements sFlow version 5. You can configure one or more FortiSwitch interfaces as sFlow agents that monitor network traffic and send sFlow datagrams containing information about traffic flow to an sFlow collector.

sFlow is normally used to provide an overall traffic flow picture of your network. You would usually operate sFlow agents on switches, routers, and firewall on your network, collect traffic data from all of them and use a collector to show traffic flows and patterns.

Syntax

```
config system sflow
   set collector-ip <collector_ipv4>
   set collector_port <port_int>
end
```

Variable	Description	Default
collector-ip <collector_ipv4>	The sFlow agents send sFlow datagrams to the sFlow collector at this IP address.	0.0.0.0
collector_port <port_int>	The UDP port number used for sending sFlow datagrams. Change this setting only if required by your sFlow collector or your network configuration. The value range is 0-65535.	6343

Example

This example shows how to configure sFlow:

```
config system sflow
```

```
   set collector-ip 20.20.20.0
   set collector_port 200
end
```

config system snmp community

Use this command to configure SNMP communities on your FortiSwitch. You add SNMP communities so that SNMP managers can connect to the system to view system information and receive SNMP traps. SNMP traps are triggered when system events occur.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the system for a different set of events. You can also the add IP addresses of up to 8 SNMP managers for each community.

Whey you configure an SNMP manager, ensure that you list it as a host in a community on the FortiSwitch that it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiSwitch, and will not be able to query it.

Syntax

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <port_number>
      set query-v1-status {enable | disable}
      set query-v2c-port <port_number>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-lport <port_number>
      set trap-v1-rport <port_number>
      set trap-v1-status {enable | disable}
      set trap-v2c-lport <port_number>
      set trap-v2c-rport <port_number>
      set trap-v2c-status {enable | disable}
      config hosts
         edit <host_number>
            set interface <if_name>
            set ip <address_ipv4>
            set source-ip <address_ipv4/mask>
         end
      config hosts6
         edit <host_number>
            set interface <if_name>
            set ip6 <address_ipv6>
            set source-ip6 <address_ipv6>
         end
      end
```

Variable	Description	Default
<index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.	No default
events <events_list>	Enable the events for which the system should send traps to the SNMP managers in this community.	All events enabled.
name <community_name>	Enter the name of the SNMP community.	No default
query-v1-port <port_number>	Enter the SNMP v1 query port number used for SNMP manager queries.	161
query-v1-status {enable | disable}	Enable or disable SNMP v1 queries for this SNMP community.	enable
query-v2c-port <port_number>	Enter the SNMP v2c query port number used for SNMP manager queries.	161
query-v2c-status {enable | disable}	Enable or disable SNMP v2c queries for this SNMP community.	enable
status {enable | disable}	Enable or disable the SNMP community.	enable
trap-v1-lport <port_number>	Enter the SNMP v1 local port number used for sending traps to the SNMP managers.	162
trap-v1-rport <port_number>	Enter the SNMP v1 remote port number used for sending traps to the SNMP managers.	162
trap-v1-status {enable | disable}	Enable or disable SNMP v1 traps for this SNMP community.	enable
trap-v2c-lport <port_number>	Enter the SNMP v2c local port number used for sending traps to the SNMP managers.	162
trap-v2c-rport <port_number>	Enter the SNMP v2c remote port number used for sending traps to the SNMP managers.	162
trap-v2c-status {enable | disable}	Enable or disable SNMP v2c traps for this SNMP community.	enable
config hosts and hosts6		
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.	No Default
interface <if_name>	Enter the name of the FortiSwitch interface to which the SNMP manager connects.	No default

Variable	Description	Default
ip <address_ipv4>	Enter the IPv4 IP address of the SNMP manager (for `hosts`).	0.0.0.0
ip6 <address_ipv6>	Enter the IPv6 IP address of the SNMP manager (for `hosts6`).	::
source-ip <address_ipv4/mask>	Enter the source IPv4 IP address for SNMP traps sent by the FortiSwitch (for `hosts`).	0.0.0.0/ 0.0.0.0
source-ip6 <address_ipv6>	Enter the source IPv6 IP address for SNMP traps sent by the FortiSwitch (for `hosts6`).	::

config system snmp sysinfo

Use this command to enable the FortiSwitch SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the system to identify it. When your SNMP manager receives traps from this FortiSwitch, you will know which system sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

Syntax

```
config system snmp sysinfo
   set contact-info <info_str>
   set description <description>
   set engine-id <engine-id_str>
   set location <location>
   set status {enable | disable}
   set trap-high-cpu-threshold <percentage>
   set trap-log-full-threshold <percentage>
   set trap-low-memory-threshold <percentage>
   set trap-temp-alarm-threshold <temperature in degrees Celsius>
   set trap-temp-warning-threshold <temperature in degrees Celsius>
end
```

Variable	Description	Default
contact-info <info_str>	Add the contact information for the person responsible for this FortiSwitch. The contact information can be up to 35 characters long.	No default
description <description>	Add a name or description of the system. The description can be up to 35 characters long.	No default

Variable	Description	Default
engine-id <engine-id_str>	Each SNMP engine maintains a value, snmpEngineID, which uniquely identifies the SNMP engine. This value is included in each message sent to or from the SNMP engine. In FortiOS, the snmpEngineID is composed of two parts: • Fortinet prefix 0x8000304404 • the optional engine-id string, 24 characters maximum, defined in this command Optionally, enter an engine-id value.	No default
location <location>	Describe the physical location of the system. The system location description can be up to 35 characters long.	No default
status {enable | disable}	Enable or disable the FortiSwitch SNMP agent.	disable
trap-high-cpu-threshold <percentage>	Enter the percentage of CPU used that will trigger the threshold SNMP trap for the high-cpu. There is some smoothing of the high CPU trap to ensure the CPU usage is constant rather than a momentary spike. This feature prevents frequent and unnecessary traps.	80
trap-log-full-threshold <percentage>	Enter the percentage of disk space used that will trigger the threshold SNMP trap for the log-full.	90
trap-low-memory-threshold <percentage>	Enter the percentage of memory used that will be the threshold SNMP trap for the low-memory.	80
trap-temp-alarm-threshold <temperature in degrees Celsius>	Set an alarm for when the system temperature reaches the specified temperature.	60
trap-temp-warning-threshold <temperature in degrees Celsius>	Set a warning for when the system temperature reaches the specified temperature. The warning threshold must be lower than the alarm threshold.	50

Example

This example shows how to set a warning and an alarm for specified system temperatures:

```
config system snmp sysinfo
   set status enable
   set trap-temp-alarm-threshold 80
   set trap-temp-warning-threshold 70
end
```

config system snmp user

Use this command to configure an SNMP user including which SNMP events the user wants to be notified about, which hosts will be notified, and if queries are enabled which port to listen on for them.

FortiSwitchOS implements the user security model of RFC 3414. You can require the user to authenticate with a password and you can use encryption to protect the communication with the user.

Syntax

```
config system snmp user
   edit <user_name>
      set queries {enable | disable}
      set query-port <port_int>
      set security-level <slevel>
   end
```

Variable	Description	Default
<user_name>	Edit or add selected user.	No default
queries {enable | disable}	Enable or disable SNMP v3 queries for this user. Queries are used to determine the status of SNMP variables.	`enable`
query-port <port_int>	Enter the number of the port used for SNMP v3 queries. If multiple versions of SNMP are being supported, each version should listen on a different port.	161
security-level <slevel>	Set the security level to one of: • **no-auth-no-priv** — no authentication or privacy • **auth-no-priv** — authentication but no privacy • **auth-priv** — authentication and privacy	no-auth-no-priv

config user

The `config user` commands provide configuration of user accounts and user groups for firewall policy authentication, administrator authentication, and some types of VPN authentication:

config user group

Use this command to add or edit user groups.

Syntax

```
config user group
   edit <group_name>
      set group-type <grp_type>
      set authtimeout <timeout>
```

```
      set http-digest-realm <attribute>
      set member <names>
      config match
         edit <match_id>
            set group-name <gname_str>
            set server-name <srvname_str>
      end
   end
```

Variable	Description	Default
<group_name>	Enter a new name to create a new group or enter an existing group name to edit that group.	No default
group-type <grp_type>	Enter the group type. `<grp_type>` determines the type of users and is one of the following: `firewall` - FortiSwitch users defined in user local, user ldap or user radius `fsso-service` - Directory Service users	firewall
authtimeout <timeout>	Set the authentication timeout for the user group, range 1 to 480 minutes. If set to 0, the global authentication timeout value is used.	0
http-digest-realm <attribute>	Enter the realm attribute for MD5-digest authentication	No default
member <names>	Enter the names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Separate the names with spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required.	No default
config match		
<match_id>	Enter an ID for the entry.	No default
group-name <gname_str>	The name of the matching group on the remote authentication server. Specify the user group names on the authentication servers that are members of this FortiSwitch user group. If no matches are specified, all users on the server can authenticate.	No default
server-name <srvname_str>	The name of the remote authentication server.	No default

Example

This example shows how to create a user group:

```
config user group
   edit "Radius_group"
      set member "FortiAuthenticator"
   end
end
```

config user ldap

Use this command to add or edit the definition of an LDAP server for user authentication.

To authenticate with the FortiSwitch, the user enters a user name and password. The system sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiSwitch. If the LDAP server cannot authenticate the user, the connection is refused by the FortiSwitch.

Syntax

```
config user ldap
edit <server_name>
   set cnid <id>
   set dn <dname>
   set group-member-check {user-attr | group-object}
   set member-attr <attr_name>
   set port <number>
   set server <domain>
   set type <auth_type>
      set username <ldap_username>
      set password <ldap_passwd>
   set password-expiry-warning {disable | enable}
   set password-renewal {disable | enable}
   set secure <auth_port>
end
```

Variable	Description	Default
<server_name>	Enter a name to identify the LDAP server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	No default
cnid <id>	Enter the common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid. Maximum 20 characters.	cn
dn <dname>	Enter the distinguished name used to look up entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the Common Name Identifier. The FortiSwitch passes this distinguished name unchanged to the server. You must provide a `dn` value if `type` is `simple`. Maximum 512 characters.	No default
group-member-check {user-attr | group-object}	Select the group membership checking method: user attribute or group object.	user-attr
member-attr <attr_name>	An attribute of the group that is used to authenticate users.	No default

Variable	Description	Default
port <number>	Enter the port number for communication with the LDAP server.	389
server <domain>	Enter the LDAP server domain name or IP address.	No default
type <auth_type>	Enter the authentication type for LDAP searches. One of: `anonymous`, `regular` or `simple` See the notes below the table for additional information.	simple
username <ldap_username>	This field is available only if `type` is `regular`. For `regular` authentication, you need a user name and password. See your server administrator for more information.	No default
password <ldap_passwd>	This field is available only if `type` is `regular`. For `regular` authentication, you need a user name and password. See your server administrator for more information.	No default
password-expiry-warning {disable | enable}	Enable or disable password expiry warnings.	disable
password-renewal {disable | enable}	Enable or disable online password renewal.	disable
secure <auth_port>{disable | starttls | ldaps}	Select the port to be used in authentication: • `disable` — port 389 • `ldaps` — port 636 • `starttls` — port 389	disable

Notes on Authentication Type

The following are the authentication types for LDAP searches:

- `anonymous` — bind using anonymous user search
- `regular` — bind using user name and password and then search
- `simple` — simple password authentication without search

You can use `simple` authentication if the user records are all under one `dn` that you know. If the users are under more than one `dn`, use the `anonymous` or `regular` type, which can search the entire LDAP database for the required user name.

If your LDAP server requires authentication to perform searches, use the `regular` type and provide values for `username` and `password`.

config user local

Use this command to add local user names and configure user authentication for the system. To add authentication by LDAP or RADIUS server you must first add servers using the `config user ldap` and

`config user radius` commands.

Syntax

```
config user local
   edit <user_name>
      set ldap-server <server_name>
      set passwd <password_str>
      set radius-server <server_name>
      set tacacs+-server <server_name>
      set status {enable | disable}
      set type <auth-type>
end
```

Variable	Description	Default
<user_name>	Enter the user name. Enter a new name to create a new user account or enter an existing user name to edit that account.	No default
ldap-server <server_name>	Enter the name of the LDAP server with which the user must authenticate. You can only select an LDAP server that has been added to the list of LDAP servers. This option is available when `type` is set to `ldap`.	No default
passwd <password_str>	Enter the password with which the user must authenticate. Passwords at least 6 characters long provide better security than shorter passwords. This option is available when `type` is set to `password`.	No default
radius-server <server_name>	Enter the name of the RADIUS server with which the user must authenticate. You can only select a RADIUS server that has been added to the list of RADIUS servers. This option is available when `type` is set to `radius`.	No default
tacacs+-server <server_name>	Enter the name of the TACACS+ server with which the user must authenticate. This option is available when `type` is set to `tacacs+`.	No default
status {enable | disable}	Enter `enable` to allow the local user to authenticate with the FortiSwitch.	enable
type <auth-type>	Enter one of the following to specify how this user's password is verified: • `ldap`: The LDAP server specified in ldap-server verifies the password. • `password`: The system verifies the password against the value of the password. • `radius`: The RADIUS server specified in radius-server verifies the password. • `tacacs+`: The TACACS+ server specified in tacacs+-server verifies the password.	No default

config user radius

Use this command to add or edit the information used for RADIUS authentication.

The default port for RADIUS traffic is 1812. If your RADIUS server is using a different port you can change the default RADIUS port. You may set a different port for each of your RADIUS servers. The maximum number of remote RADIUS servers that can be configured for authentication is 10.

The RADIUS server is now provided with more information to make authentication decisions, based on values in `server`, `nas-ip`, and the `config user group` subcommand `config match`. Attributes include:

- **NAS-IP-Address** — RADIUS setting or IP address of FortiSwitch interface used to talk to RADIUS server, if not configured
- **NAS-Port** — physical interface number of the traffic that triggered the authentication
- **Called-Station-ID** — same value as NAS-IP Address but in text format
- **Fortinet-Vdom-Name** — name of VDOM of the traffic that triggered the authentication
- **NAS-Identifier** — configured hostname in non-HA mode; HA cluster group name in HA mode
- **Acct-Session-ID** — unique ID identifying the authentication session
- **Connect-Info** — identifies the service for which the authentication is being performed (web-auth, vpn-ipsec, vpn-pptp, vpn-l2tp, vpn-ssl, admin-login, test)

You can select an alternative authentication method for each server. These include CHAP, PAP, MS-CHAP, and MS-CHAP-v2.

Syntax

```
config user radius
   edit <RADIUS_user_name>
      set acct-interim-interval <seconds>
      set all-usergroup {enable | disable}
      set auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}
      set nas-ip <use_ip>
      set radius-coa {enable | disable}
      set radius-port <radius_port_num>
      set secret <server_password>
      set server <domain>
      set source-ip <ipv4_addr>
      config acct-server
         edit <accounting_server_ID>
            set status {enable | disable}
            set server <accounting_server_ipv4_addr>
            set secret <accounting_server_secret>
            set port <accounting_server_port>
            set source-ip <acccounting_source_ip>
   end
```

Variable	Description	Default
<server_name>	Enter a name of the RADIUS user group. Enter a new name to create a new group definition or enter an existing group name to edit that group definition.	No default

Variable	Description	Default
acct-interim-interval <seconds>	Enter the number of seconds between each interim accounting message sent to the RADIUS server. The value range is 60-86400.	600
all-usergroup {enable | disable}	Enable to automatically include this RADIUS server in all user groups.	disable
auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}	Select the authentication method for this RADIUS server. auto uses pap, ms_chap_v2, and chap.	auto
nas-ip <use_ip>	IP address used as NAS-IP-Address and Called-Station-ID attribute in RADIUS access requests. RADIUS setting or IP address of FGT interface used to talk with RADIUS server, if not configured.	No default
radius-coa {enable | disable}	Enable or disable whether this server will use RADIUS change of authorization (CoA).	disable
radius-port <radius_port_num>	Change the default RADIUS port for this server. Range is 0-65535	1812
secret <server_password>	Enter the RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length.	No default
server <domain>	Enter the RADIUS server domain name or IP address.	No default
source-ip <ipv4_addr>	Enter the source IP for communications to RADIUS server.	0.0.0.0
config acct-server		
<accounting_server_ID>	Enter the identifier for the accounting server. The value range is 0-4294967295.	No default
status {enable | disable}	Enable or disable RADIUS accounting.	disable
server <accounting_server_ipv4_addr>	Enter the IPv4 address of the RADIUS server that will be receiving the accounting messages.	No default
secret <accounting_server_secret>	Enter the shared secret key for the RADIUS accounting server.	*
port <accounting_server_port>	Enter the port number for the RADIUS accounting server to receive accounting messages from the FortiSwitch.	1813
source-ip <acccounting_source_ip>	Enter the IPv4 address of the server that will be sending accounting messages.	0.0.0.0

Notes on context timeout

The number of seconds that a user context entry can remain in the user context list without the system receiving a communication session from the carrier end point. If a user context entry is not being looked up, then the user must no longer be connected to the network.

This timeout is only required if the system doesn't receive the RADIUS Stop record. However, even if the accounting system does send RADIUS Stop records this timeout should be set in case the FortiSwitch misses a Stop record.

The default user context entry timeout is 28800 seconds (8 hours). You can keep this timeout relatively high because its not usually a problem to have a long list, but entries that are no longer used should be removed regularly.

You might want to reduce this timeout if the accounting server does not send RADIUS Stop records. Also if customer IP addresses change often you might want to set this timeout lower so that out of date entries are removed from the list.

If this timeout is too low the FortiSwitch could remove user context entries for users who are still connected.

Set the timeout to 0 if you do not want the FortiSwitch to remove entries from the list except in response to RADIUS Stop messages.

Dynamic Flag values:

`none` — Disable writing event log messages for dynamic profile events.

`accounting-event` — Enable to write an event log message when the system does not find the expected information in a RADIUS Record. For example, if a RADIUS record contains more than the expected number of addresses.

`accounting-stop-missed` — Enable to write an event log message whenever a user context entry timeout expires indicating that the system removed an entry from the user context list without receiving a RADIUS Stop message.

`context-missing` — Enable to write an event log message whenever a user context creation timeout expires indicating that the system was not able to match a communication session because a matching entry was not found in the user context list.

`profile-missing` — Enable to write an event log message whenever the system cannot find a profile group name in a RADIUS start message that matches the name of a profile group added to the system.

`protocol-error` — Enable to write an event log message if RADIUS protocol errors occur. For example, if a RADIUS record contains a RADIUS secret that does not match the one added to the dynamic profile.

`radiusd-other` — Enable to write event log messages for other events. The event is described in the log message. For example, write a log message if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.

Example

This example shows how to set up RADIUS accounting:

```
config user radius
   edit "local-RADIUS"
      set server 10.0.23.5
      set secret djfhde;rkjfkrekdfjeke
```

```
      set auth-type ms_chap_v2
      set acct-interim-interval 1200
      config acct-server
         edit 1
            set status enable
            set server 10.0.23.5
            set secret djfhde;rkjfkrekdfjeke
            set port 1813
            set source-ip 10.105.142.19
         next
      end
   next
end
```

config user setting

Use this command to change user authorization settings.

Syntax

```
config user setting
   set auth-blackout-time <blackout_time_int>
   set auth-cert <cert_name>
   set auth-http-basic {disable | enable}
   set auth-invalid-max <int>
   set auth-multi-group {enable | disable}
   set auth-secure-http {enable | disable}
   set auth-type {ftp | http | https | telnet}
   set auth-timeout <auth_timeout_minutes>
   set auth-timeout-type {idle-timeout | hard-timeout | new-session}
   config auth-ports
      edit <auth-table-entry-id>
         set port <port_int>
         set type {ftp | http | https | telnet}
      end
   end
```

Variable	Description	Default
auth-blackout-time <blackout_time_int>	When a firewall authentication attempt fails 5 times within one minute the IP address that is the source of the authentication attempts is denied access for the <blackout_time_int> period in seconds. The range is 0 to 3600 seconds.	0
auth-cert <cert_name>	HTTPS server certificate for policy authentication. Fortinet_Factory, Fortinet_Firmware (if applicable to your FortiSwitch), and self-sign are built-in certificates but others will be listed as you add them.	self-sign

Variable	Description	Default
auth-http-basic {disable | enable}	Enable or disable support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of displaying an authentication web page. Some basic web browsers, for example, web browsers on mobile devices, may only support HTTP basic authentication.	disable
auth-invalid-max <int>	Enter the maximum number of failed authentication attempts to allow before the client is blocked. Range: 1-100.	5
auth-multi-group {enable | disable}	This option can be disabled if the Active Directory structure is setup such that users belong to only 1 group for purpose of firewall authentication.	enable
auth-secure-http {enable | disable}	Enable to have http user authentication redirected to secure channel - https.	disable
auth-type {ftp | http | https | telnet}	Set the user authentication protocol support for firewall policy authentication. User controls which protocols should support the authentication challenge.	No Default
auth-timeout <auth_timeout_minutes>	Set the number of minutes before the firewall user authentication timeout requires the user to authenticate again. The maximum authtimeout interval is 480 minutes (8 hours). To improve security, keep the authentication timeout at the default value of 5 minutes.	5
auth-timeout-type {idle-timeout | hard-timeout | new-session}	Set the type of authentication timeout. `idle-timeout` — applies only to idle session `hard-timeout` — applies to all sessions `new-session` — applies only to new sessions	idle-timeout
config auth-ports		
<auth-table-entry-id>	Create an entry in the authentication port table if you are using non-standard ports.	No Default
port <port_int>	Specify the authentication port. Range 1 to 65535.	1024
type {ftp | http | https | telnet}	Specify the protocol to which `port` applies.	http

config user tacacs+

Use this command to add or edit the information used for TACACS+ authentication.

Syntax

```
config user tacacs+
   edit <user name>
      set authen-type {ascii | auto | chap | mschap | pap}
      set authorization {enable | disable}
      set key <passwd>
      set port <port number>
      set server <domain>
      set source-ip <ipv4_addr>
```

Variable	Description	Default
<user name>	Enter the name of the user.	No default
authen-type{ascii | auto | chap | mschap | pap}	Set the authentication type. Auto will use PAP, MSCHAP, and CHAP (in that order).	auto
authorization {disable | enable}	Enable TACACS+ authorization (service=fortigate)	disable
key <passwd>	Password value for the server.	*
port <port_int>	Specify the authentication port. Range 1 to 65535.	49
server <domain>	Specify the domain name of the server	No default
source-ip <ipv4_addr>	Set the source IP address.	0.0.0.0

Example

This example shows how to configure a TACACS user account for login authentication::

```
config user tacacs+
   edit tacserver
      set authen-type ascii
      set authorization enable
      set key temporary
      set server tacacs_server
   end
```

diagnose

Use the `diagnose` commands to help with troubleshooting:

diagnose bpdu-guard display status

Use this command to display the status of the spanning tree protocol (STP) bridge protocol data unit (BPDU) guard:

```
diagnose bpdu-guard display status
```

To configure STP BPDU guard, see config switch interface on page 54.

Example output

```
Portname              State      Status       Timeout(m)     Count    Last-Event
__________________    _______    _________    ___________    _____    ______________

port1                 disabled     -              -              -            -
port2                 disabled     -              -              -            -
port3                 disabled     -              -              -            -
port4                 disabled     -              -              -            -
port5                 disabled     -              -              -            -
port6                 disabled     -              -              -            -
port9                 disabled     -              -              -            -
port10                disabled     -              -              -            -
port11                disabled     -              -              -            -
port12                disabled     -              -              -            -
port13                disabled     -              -              -            -
port14                disabled     -              -              -            -
port15                disabled     -              -              -            -
port16                disabled     -              -              -            -
port17                disabled     -              -              -            -
port18                disabled     -              -              -            -
port19                disabled     -              -              -            -
port20                disabled     -              -              -            -
port21                disabled     -              -              -            -
port22                disabled     -              -              -            -
port23                disabled     -              -              -            -
port24                disabled     -              -              -            -
port25                disabled     -              -              -            -
port26                disabled     -              -              -            -
port27                disabled     -              -              -            -
port28                disabled     -              -              -            -
port29                disabled     -              -              -            -
port30                enabled      -              60             0            -
```

diagnose debug application

Use this command to set the debug level for application daemons. Some applications must be set to level 8 or higher to enable output for other diagnose debug commands. If you do not specify the debugging level, the current debbuging level is returned.

```
diagnose debug application <application> [<debugging_level>]
```

The following applications are supported:

- authd — Authentication daemon
- bfdd — BFD daemon
- ctrld — General FortiSwitch control daemon
- cu_swtpd — Switch-controller CAPWAP control daemon
- dhcpc — DHCP client module
- dhcprelay — DHCP relay daemon
- dhcps — DHCP server
- dnsproxy — DNS proxy module
- eap_proxy — EAP proxy daemon
- fdpd — Fortinet Discovery Protocol (FDP) daemon
- fgd_alert — FortiGuard alert messages
- flgd — Switch-controller configuration daemon
- fnbamd — FortiGate nonblocking authentication daemon
- fortilinkd — FortiLink daemon
- fpmd —Hardware offload daemon
- fsmgr — FortiSwitch manager daemon
- httpsd — HTTPS daemon
- igmp_snooping — IGMP snooping debugging
- ip6addrd — IPv6 address utility
- ipconflictd — IP conflict detection daemon
- l2d — Daemon for layer-2 features
- l2dbg — Daemon for hardware-related operations needed by layer 2
- l3 — Layer-3 debugging
- lacpd — LACP daemon
- libswitchd — FortiSwitch library daemon
- link-monitor — Link monitor daemon
- lldpmedd — LLPD-MED daemon
- miglogd — Logging daemon
- ntpd — NTP daemon
- nwmcfgd — Daemon for network-monitoring configuration
- nwmonitord — Packet-handling and parsing daemon for network monitoring
- ospfd — OSPF routing daemon
- radiusd — RADIUS daemon
- ripd — RIP routing daemon
- router-launcher — Daemon for launching the routing system
- rsyslogd — RSYSLOG daemon
- sflowd — sFlow protocol module
- snmpd — SNMP daemon
- sshd — SSH daemon
- stpd — STP daemon
- switch-launcher — Daemon for launching the FortiSwitch system

- trunkd — Trunk daemon
- vrrpd —VRRP daemon
- wiredap — Daemon for 802.1X port-based authentication
- zebra — Core router daemon

Example output

```
S524DF4K15000024 # diagnose debug application flgd

flgd debug level is 8 (0x8)
```

diagnose debug authd

Use these commands to manage the authentication daemon:

```
diagnose debug authd clear
diagnose debug authd fsso clear-logons
diagnose debug authd fsso filter clear
diagnose debug authd fsso filter group <group_name>
diagnose debug authd fsso filter server <FSSO_agent_name>
diagnose debug authd fsso filter source <IPv4_address> <IPv4_address>
diagnose debug authd fsso filter user <user_name>
diagnose debug authd fsso list
diagnose debug authd fsso refresh-groups
diagnose debug authd fsso refresh-logons
diagnose debug authd fsso server-status
diagnose debug authd fsso summary
```

Variable	Description
clear	Delete internal data structures and keepalive sessions.
fsso clear-logons	Delete Fortinet Single Sign on (FSSO) logon information.
fsso filter clear	Delete all FSSO filters.
fsso filter group <group_name>	List only the logons by the specified FSSO group.
fsso filter server <FSSO_agent_name>	List only the logons for the specified FSSO agent.
fsso filter source <IPv4_address> <IPv4_address>	List only the logons for the specified range of IPv4 addresses.
fsso filter user <user_name>	List only the logons by the specified user.
fsso list	Display the current FSSO logons.
fsso refresh-groups	Refresh the FSSO group mappings.

Variable	Description
fsso refresh-logons	Synchronize the FSSO logon database.
fsso server-status	Display the status of the FSSO agent connection.
fsso summary	Display a summary of current FSSO logons.

Example output

```
diag debug authd fsso server-status

Server Name     Connection Status     Version
-----------     -----------------     -------
fsso            connected             FSSO 5.0.0237

diagnose debug authd fsso list
IP: 10.1.1.5  User: ADM_FWCHECK  Groups: FW_OPERATORS/ADMINISTRATORS
```

diagnose debug cli

Use this command to set or find the debug level for the CLI:

```
diagnose debug cli [<0-8>]
```

Example output

```
S524DF4K15000024 # diagnose debug cli

Cli debug level is 8
```

diagnose debug config-error-log

Use this command to display information about the configuration error log:

```
diagnose debug config-error-log {clear | read}
```

Variable	Description
clear	Clear the configuration error log.
fsso	Display configuration errors on the console.

diagnose debug console

Use these commands to display information about the console:

```
diagnose debug console no-user-log-msg {enable | disable}
```

```
diagnose debug console send <AT command>
diagnose debug console timestamp {enable | disable}
```

Variable	Description
no-user-log-msg {enable | disable}	Enable or disable the display of user log messages on the console.
send <AT command>	Send out the specified modem AT command.
timestamp {enable | disable}	Enable or disable the time stamp.

diagnose debug crashlog

Use this command to display or erase the crash log:

```
diagnose debug crashlog {clear | get}
```

Variable	Description
clear	Clear the crash log.
get	Display the crash log on the console.

Example output

```
S524DF4K15000024 # diagnose debug crashlog get

Rk9SVP94nDK0NLPUNTTSNTZUMDSzMjCwMjVXSErOjc9IzEvJSY3PTM8tKI5Pzk2x
UvB1dgwO0Q1xdPJx1Q32jHK1MjQwMuECCCAjA0NzXQNLXQMzBUOgZgMrQ0uFkoxU
hezMnJzUFIWUxNTc/DyFzGIF/aTMPP301JKSSiuF4pLEktJiW4MKAy6AAELWb2gF
dIKJKUn6AQIIVb+JmZWpCUn6AQIIWb+RlYGxlbExSfoBAghZv7GVqamVEWn+Bwgg
ZP0mVgYWwCAkST9AAKHqNzQHxR8p+gECCFW/MdALhiToN+ICCCA0/WZWxqTpBwgg
ZP3AwDMGJkGS3A8QQKj6TYBJwIIk/QABhKbfBBiFJLkfIIDQ9JtaGZNivxEXQAAh
6zcDxb8RafEHEECo+oH+NyAt/QMEEKp+UP41Ikk/QADB9ZuD8r+RpRXQIOL1GxsY
cAEEEKoJphakpgCAAELWbwgKQQPSQhAggFD1A3OAMWkhABBAaPotrUxIsx8ggJD1
A0sgU1JzMEAAIesHZl8jICJJP0AAIesHpgBz0koAAy6AAELWb24FTgQk6QcIIFT9
JkD3k5KCDLgAAghNPzD+SbMfIIBQ9ZsaAyshkvQDBBCyfqDlwEKYtBIIIBQ9QOj
0IS08AcIIDT9ZqSlHyMugABC1W8EDH/SakCAAELVD8w/JMY/QAAh6wcWH0bAJECS
foAAguu3UDAwtzIClmCklB+gEggggJBNsLQCV8MkuQAggND0A+sA0lIQQACh6jcC
1mGklYAAAYSkH1gCGZkCnUCSfoAAQtUPKgFJsx8ggFD1mwBzEGklGEAAoek3AUYi
...
```

diagnose debug disable

Use this command to disable debugging output:

```
diagnose debug disable
```

diagnose debug enable

Use this command to enable debugging output:

```
diagnose debug enable
```

diagnose debug info

Use this command to display the debugging level:

```
diagnose debug info
```

Example output

```
S524DF4K15000024 # diagnose debug info
debug output:           enable
console timestamp:      disable
console no user log message:    disable
fsmgr debug level:      16 (0x10)
CLI debug level:        8
```

diagnose debug kernel level

Use this command to display or set the debugging level for the kernel:

```
diagnose debug kernel level [<integer>]
```

Example output

```
S524DF4K15000024 # diagnose debug kernel level

Kernel debug level is 0
```

diagnose debug packet_test

Use this command to display a report about the specified port for technical support:

```
diagnose debug packet_test <port_ID>
```

Example output

```
S524DF4K15000024 # diagnose debug packet_test 30

RX: port:0(tx port 30) len:0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

RX: port:0(tx port 30) len:0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
Send: 2, Recv: 2
```

diagnose debug port-mac

Use this command to display the mapping between MAC addresses and ports:

```
diagnose debug port-mac {check-mac | list}
```

Variable	Description
check-mac	Check to see if the specified MAC address is valid.
list	List the mapping between MAC addresses and ports.

Example output

```
S524DF4K15000024 # diagnose debug port-mac check-mac 08:5b:0e:f1:95:e4
Input MAC address 08:5b:0e:f1:95:e4 found in range
08:5b:0e:e5:4f:d6--08:5b:0e:f1:9b:a4
90:6c:ac:30:19:22--90:6c:ac:7b:d6:d0
Allocated split-port MAC for port 32 is  00:00:00:00:00:00.

S524DF4K15000024 # diagnose debug port-mac list
Base MAC: 08:5b:0e:f1:95:e4

Port Name             Port #           Split Port Idx          MAC
================================================================================
       port1                  1                        0          08:5b:0e:f1:95:e6
       port2                  2                        0          08:5b:0e:f1:95:e7
       port3                  3                        0          08:5b:0e:f1:95:e8
       port4                  4                        0          08:5b:0e:f1:95:e9
       port5                  5                        0          08:5b:0e:f1:95:ea
       port6                  6                        0          08:5b:0e:f1:95:eb
       port7                  7                        0          08:5b:0e:f1:95:ec
       port8                  8                        0          08:5b:0e:f1:95:ed
       port9                  9                        0          08:5b:0e:f1:95:ee
       port10                 10                       0          08:5b:0e:f1:95:ef
       port11                 11                       0          08:5b:0e:f1:95:f0
       port12                 12                       0          08:5b:0e:f1:95:f1
       port13                 13                       0          08:5b:0e:f1:95:f2
       port14                 14                       0          08:5b:0e:f1:95:f3
       port15                 15                       0          08:5b:0e:f1:95:f4
       port16                 16                       0          08:5b:0e:f1:95:f5
       port17                 17                       0          08:5b:0e:f1:95:f6
       port18                 18                       0          08:5b:0e:f1:95:f7
       port19                 19                       0          08:5b:0e:f1:95:f8
       port20                 20                       0          08:5b:0e:f1:95:f9
       port21                 21                       0          08:5b:0e:f1:95:fa
       port22                 22                       0          08:5b:0e:f1:95:fb
```

```
        port23              23                  0          08:5b:0e:f1:95:fc
        port24              24                  0          08:5b:0e:f1:95:fd
        port25              25                  0          08:5b:0e:f1:95:fe
        port26              26                  0          08:5b:0e:f1:95:ff
        port27              27                  0          08:5b:0e:f1:96:00
        port28              28                  0          08:5b:0e:f1:96:01
        port29              29                  0          08:5b:0e:f1:96:02
        port30              30                  0          08:5b:0e:f1:96:03
        internal            31                  0          08:5b:0e:f1:95:e4
```

diagnose debug report

Use this command to display a detailed debugging report for technical support:

```
diagnose debug report
```

Example output

```
S524DF4K15000024 # diagnose debug report

Version: FortiSwitch-524D-FPOE v3.6.3,build0390,171020 (GA)
Serial-Number: S524DF4K15000024
BIOS version: 04000013
System Part-Number: P18045-04
Burn in MAC: 08:5b:0e:f1:95:e4
Hostname: S524DF4K15000024
Distribution: International
Branch point: 390
System time: Tue Jan  6 13:53:02 1970

------------------------------------------------------------------
Serial Number: S524DF4K15000024   Diagnose output
------------------------------------------------------------------

### get system status

CPU states: 0% user 4% system 0% nice 96% idle
Memory states: 10% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30
minutes
Uptime: 5 days,  21 hours,  53 minutes

### get system performance status

config system interface
edit "mgmt"
set ip 192.168.1.99 255.255.255.0
set allowaccess ping https ssh
set type physical
set snmp-index 33
next
edit "internal"
```

```
set type physical
set snmp-index 32
next
end

### show system interface

### show router static

### diagnose ip address list
...'
```

diagnose debug reset

Use this command to reset all debugging levels to the default levels:

```
diagnose debug reset
```

diagnose flapguard instance status

Use this command to get flap-guard information for all switch ports:

```
diagnose flapguard instance status
```

Example output

```
S524DF4K15000024 # diagnose  flapguard instance status

Portname   Status       flap-rate    flap-duration   flaps/duration  Last-Event
_________  _______      _________    _____________   ______________  ___________

port1         -              5             30               0           -
port2         -              5             30               0           -
port3         -              5             30               0           -
port4         -              5             30               0           -
port5         -              5             30               0           -
port6         -              5             30               0           -
port7         -              5             30               0           -
port8         -              5             30               0           -
port9         -              5             30               0           -
port10        -              5             30               0           -
port11        -              5             30               0           -
port12        -              5             30               0           -
port13        -              5             30               0           -
port14        -              5             30               0           -
port15        -              5             30               0           -
port16        -              5             30               0           -
port17        -              5             30               0           -
port18        -              5             30               0           -
port19        -              5             30               0           -
```

```
port20          -               5               30              0               -
port21          -               5               30              0               -
port22          -               5               30              0               -
port23          -               5               30              0               -
port24          -               5               30              0               -
port25          -               5               30              0               -
port26          -               5               30              0               -
port27          -               5               30              0               -
port28          -               5               30              0               -
port29          -               5               30              0               -
port30          -               5               30              0               -
```

diagnose hardware

Use these commands to diagnose the hardware. You must be logged in as a super user for these commands.

```
diagnose hardware certificate
diagnose hardware deviceinfo
diagnose hardware ioport {byte <value> | long <arguments> | word <arguments>}
diagnose hardware ipsec
diagnose hardware pciconfig
diagnose hardware sysinfo
```

Variable	Description
certificate	Verify which certificates are present on the FortiSwitch and that all installed certificates are valid.
deviceinfo	Get device information.
ioport {byte <value> | long <arguments> | word <arguments>}	Read and write data using the input/output port.
ipsec	Get information about the ASIC's Internet Protocol Security (IPSec).
pciconfig	Get payment card industry (PCI) information.
sysinfo	Get system information.

Example output

```
S524DF4K15000024 # diagnose hardware certificate

Checking Fortinet_CA.cer integrality ........Passed
Checking Fortinet_Factory.cer integrality ........Passed
Checking Fortinet_Factory.cer key-pair integrality ........Passed
Checking Fortinet_Factory.cer Serial-No. ........Passed
Checking Fortinet_Factory.cer timeliness ........Passed
Checking Fortinet_Factory.key integrality ........Passed
Checking Fortinet_CA2.cer existent ........[Not Exist]
```

```
Checking Fortinet_Factory2.cer existent ........[Not Exist]
Checking Fortinet_Factory2.key existent ........[Not Exist]
```

diagnose ip address

Use these commands to manage IP addresses:

```
diagnose ip address add <interface_name> <IPv4_address> <IP_network_mask>
diagnose ip address delete <interface_name> <IPv4_address>
diagnose ip address flush
diagnose ip address list
```

Variable	Description
add <interface_name> <IPv4_ address> <IP_network_mask>	Add an IPv4 address to the specified interface.
delete <interface_name> <IPv4_ address>	Delete an IPv4 address from the specified interface.
flush	Delete all IP addresses.
list	List all IP addresses and which interfaces they are assigned to.

Example output

```
S524DF4K15000024 # diagnose ip address list

IP=127.0.0.1->127.0.0.1/255.0.0.0 index=1 devname=lo
IP=192.168.1.99->192.168.1.99/255.255.255.0 index=2 devname=mgmt
IP=10.105.19.3->10.105.19.3/255.255.252.0 index=2 devname=mgmt
IP=170.38.65.1->170.38.65.1/255.255.255.0 index=71 devname=vlan35
IP=180.1.1.1->180.1.1.1/255.255.255.0 index=72 devname=vlan85
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=73 devname=int1
IP=10.10.10.1->10.10.10.1/255.255.255.0 index=74 devname=vlan-8
IP=11.1.1.100->11.1.1.100/255.255.255.255 index=74 devname=vlan-8
```

diagnose ip arp

Use these commands to manage the Address Resolution Protocol (ARP) table:

```
diagnose ip arp add <interface_name> <IPv4_address> <MAC_address>
diagnose ip arp delete <interface_name> <IPv4_address>
diagnose ip arp flush <interface_name>
diagnose ip arp list
```

Variable	Description
arp add <interface_name> <IPv4_address>	Add an Address Resolution Protocol (ARP) entry for the IP address on the specified interface.
arp delete <interface_name> <IPv4_address>	Delete an Address Resolution Protocol (ARP) entry for the IP address on the specified interface.
arp flush <interface_name>	Delete the ARP table for the specified interface.
arp list	Display the ARP table.

Example output

```
S524DF4K15000024 # diagnose ip arp list

index=2 ifname=mgmt 10.105.16.1 90:6c:ac:15:2f:94 state=00000002 use=117606 con-
firm=537 update=67371 ref=1
index=70 ifname=internal 192.168.0.10 state=00000001 use=24 confirm=178601 update-
e=124 ref=1
index=74 ifname=vlan-8 11.1.1.100 00:00:5e:00:01:05 (proxy)
```

diagnose ip route

Use these commands to manage static routes and the routing table:

```
diagnose ip route add <interface_name> <IPv4_address> <IP_network_mask>
diagnose ip route delete <interface_name> <IPv4_address>
diagnose ip route flush
diagnose ip route list [<arguments>]
diagnose ip route verify <interface_name> <IPv4_address> <IP_network_mask>
```

Variable	Description
add <interface_name> <IPv4_address> <IP_network_mask>	Add a static route to the specified interface.
delete <interface_name> <IPv4_address>	Delete a static route from the specified interface.
flush	Delete the routing table.
list [<arguments>]	Display the routing table.
verify <interface_name> <IPv4_address> <IP_network_mask>	Verify a static route on the specified interface.

Example output

```
S524DF4K15000024 # diagnose ip route list

tab=254 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0
gwy=10.105.16.1 dev=2(mgmt)
tab=254 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.10.10.0/24 pre-
f=10.10.10.1 gwy=0.0.0.0 dev=74(vlan-8)
tab=254 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.105.16.0/22 pre-
f=10.105.19.3 gwy=0.0.0.0 dev=2(mgmt)
tab=254 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->39.3.2.0/24 pref=0.0.0.0
gwy=180.1.1.2 dev=72(vlan85)
tab=254 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->170.38.65.0/24 pre-
f=170.38.65.1 gwy=0.0.0.0 dev=71(vlan35)
tab=254 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->180.1.1.0/24 pre-
f=180.1.1.1 gwy=0.0.0.0 dev=72(vlan85)
tab=254 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0->192.168.1.0/24 pre-
f=192.168.1.99 gwy=0.0.0.0 dev=2(mgmt)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.10.10.0/32 pre-
f=10.10.10.1 gwy=0.0.0.0 dev=74(vlan-8)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.10.10.1/32 pre-
f=10.10.10.1 gwy=0.0.0.0 dev=74(vlan-8)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.10.10.255/32 pre-
f=10.10.10.1 gwy=0.0.0.0 dev=74(vlan-8)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.105.16.0/32 pre-
f=10.105.19.3 gwy=0.0.0.0 dev=2(mgmt)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.105.19.3/32 pre-
f=10.105.19.3 gwy=0.0.0.0 dev=2(mgmt)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->10.105.19.255/32 pre-
f=10.105.19.3 gwy=0.0.0.0 dev=2(mgmt)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->11.1.1.100/32 pre-
f=11.1.1.100 gwy=0.0.0.0 dev=74(vlan-8)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.0.0.0/32 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=1(lo)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.0.0.0/32 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=73(int1)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.0.0.0/8 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=1(lo)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.0.0.0/8 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=73(int1)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.0.0.1/32 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=1(lo)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.0.0.1/32 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=73(int1)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.255.255.255/32 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=1(lo)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->127.255.255.255/32 pre-
f=127.0.0.1 gwy=0.0.0.0 dev=73(int1)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->170.38.65.0/32 pre-
f=170.38.65.1 gwy=0.0.0.0 dev=71(vlan35)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->170.38.65.1/32 pre-
f=170.38.65.1 gwy=0.0.0.0 dev=71(vlan35)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->170.38.65.255/32
```

```
pref=170.38.65.1 gwy=0.0.0.0 dev=71(vlan35)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->180.1.1.0/32 pre-
f=180.1.1.1 gwy=0.0.0.0 dev=72(vlan85)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->180.1.1.1/32 pre-
f=180.1.1.1 gwy=0.0.0.0 dev=72(vlan85)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->180.1.1.255/32 pre-
f=180.1.1.1 gwy=0.0.0.0 dev=72(vlan85)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->192.168.1.0/32 pre-
f=192.168.1.99 gwy=0.0.0.0 dev=2(mgmt)
tab=255 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0->192.168.1.99/32 pre-
f=192.168.1.99 gwy=0.0.0.0 dev=2(mgmt)
tab=255 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0->192.168.1.255/32 pre-
f=192.168.1.99 gwy=0.0.0.0 dev=2(mgmt)
```

diagnose ip router bfd

NOTE: To enable bidirectional forwarding detection (BFD) debugging, you must use the `diagnose debug application bfdd` to set the debugging level to 8 or higher. To configure BFD, see config system interface on page 101.

Use these commands to manage BFD debugging:

```
diagnose ip router bfd cpu-usage show
diagnose ip router bfd debug all {enable | disable}
diagnose ip router bfd debug fsm {enable | disable}
diagnose ip router bfd debug net {enable | disable}
diagnose ip router bfd debug show
diagnose ip router bfd debug zebra {enable | disable}
diagnose ip router bfd memory-usage show
diagnose ip router bfd work-queues show
```

Variable	Description
cpu-usage show	Display statistics for CPU usage.
debug all {enable | disable}	Enable or disable all BFD debugging.
debug fsm {enable | disable}	Enable or disable BFD FortiGate Storage Modules (FSM) debugging.
debug net {enable | disable}	Enable or disable BFD network debugging.
debug show	Display the BFD debugging level and which kinds of BFD debugging are enabled.
debug zebra {enable | disable}	Enable or disable communication with the core router daemon.
memory-usage show	Display statistics for memory usage.
work-queues show	Display information about work queues.

Example output

```
S524DF4K15000024 # diagnose ip router bfd cpu-usage show
                     CPU (user+system): Real (wall-clock):
Runtime(ms)   Invoked Avg uSec Max uSecs Avg uSec Max uSecs  Type  Thread
       0.000         1        0         0      181       181    E   zclient_connect
       0.000        91        0         0       64       125 R      zclient_read
       0.000        26        0         0       40        82  W     vty_flush
       0.000        26        0         0       93       200 R      vty_read
       0.000         4        0         0      104       168 R      vty_accept
       0.000       148        0         0       66       200 RWTEXB TOTAL

S524DF4K15000024 # diagnose ip router bfd debug fsm enable
2017/09/19 20:21:44 BFD: Vty connection from 127.0.0.1
2017/09/19 20:21:44 BFD: Vty connection from 127.0.0.1
New debugging state:
Note: "diagnose debug application bfdd" needs to be set to 8 or higher
Current level: 8
BFD debugging status:
debug bfd zebra
debug bfd fsm
debug bfd net

S524DF4K15000024 # diagnose ip router bfd debug net enable
2017/09/19 20:25:17 BFD: Vty connection from 127.0.0.1
2017/09/19 20:25:17 BFD: Vty connection from 127.0.0.1
New debugging state:
Note: "diagnose debug application bfdd" needs to be set to 8 or higher
Current level: 8
BFD debugging status:
debug bfd zebra
debug bfd fsm
debug bfd net

S524DF4K15000024 # diagnose ip router bfd debug show
2017/09/19 20:27:27 BFD: Vty connection from 127.0.0.1
Note: "diagnose debug application bfdd" needs to be set to 8 or higher
Current level: 8
BFD debugging status:
debug bfd zebra
debug bfd fsm
debug bfd net

S524DF4K15000024 # diagnose ip router bfd debug zebra enable
2017/09/19 20:29:20 BFD: Vty connection from 127.0.0.1
2017/09/19 20:29:20 BFD: Vty connection from 127.0.0.1
New debugging state:
Note: "diagnose debug application bfdd" needs to be set to 8 or higher
Current level: 8
BFD debugging status:
debug bfd zebra
debug bfd fsm
debug bfd net
```

```
S524DF4K15000024 # diagnose ip router bfd memory-usage show
2017/09/19 20:34:07 BFD: Vty connection from 127.0.0.1
System allocator statistics:
Total heap allocated:  132 KiB
Holding block headers: 0 bytes
Used small blocks:     0 bytes
Used ordinary blocks:  76 KiB
Free small blocks:     776 bytes
Free ordinary blocks:  56 KiB
Ordinary blocks:       4
Small blocks:          48
Holding blocks:        0
(see system documentation for 'mallinfo' for meaning)
-----------------------------
Temporary memory              :          1
String vector                 :          3
Vector                        :        134
Vector index                  :        134
Link List                     :         79
Link Node                     :         90
Thread                        :         12
Thread master                 :          1
Thread stats                  :          5
VTY                           :          2
VTY history                   :          1
Interface                     :         76
Connected                     :         14
Buffer                        :          2
Buffer data                   :          1
Stream                        :          2
Stream data                   :          2
Prefix                        :         19
Hash                          :          2
Hash Bucket                   :          5
Hash Index                    :          2
Route table                   :          2
Command desc                  :       1218
Logging                       :          1
Zclient                       :          1
Priority queue                :          2
Priority queue data           :          2
Host config                   :          5
-----------------------------
BFD instance                  :          1
BFD lport                     :          1
BFD table pointer             :          2
BFD neighbor table            :          1
-----------------------------
BFD interface                 :         76
```

diagnose ip router command

Use these commands to send commands to various daemons:

```
diagnose ip router command bfd {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command ospf {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command rip {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command zebra {cmd <arguments>| cmd-conf-term <arguments>}
```

Variable	Description
bfd {cmd <arguments>| cmd-conf-term <arguments>}	Send commands to the BFD daemon in enable mode (`cmd`) or in configure terminal mode (`cmd-conf-term`).
ospf {cmd <arguments>| cmd-conf-term <arguments>}	Send commands to the OSPF daemon in enable mode (`cmd`) or in configure terminal mode (`cmd-conf-term`).
rip {cmd <arguments>| cmd-conf-term <arguments>}	Send commands to the RIP daemon in enable mode (`cmd`) or in configure terminal mode (`cmd-conf-term`).
zebra {cmd <arguments>| cmd-conf-term <arguments>}	Send commands to the core router daemon in enable mode (`cmd`) or in configure terminal mode (`cmd-conf-term`).

diagnose ip router launch-info show

Use this command to display information about the process launch of the BFD daemon, OSPF daemon, RIP daemon, and core routing daemon:

```
diagnose ip router launch-info show
```

Example output

```
S524DF4K15000024 # diagnose ip router launch-info show

/bin/zebra Pid: 770 Ready: 0x1 NumRestart: 0
/bin/ospfd Pid: 824 Ready: 0x1 NumRestart: 0
/bin/bfdd Pid: 825 Ready: 0x1 NumRestart: 0
/bin/ripd Pid: 826 Ready: 0x1 NumRestart: 0
```

diagnose ip router ospf

NOTE: To enable open shortest path first (OSPF) debugging, you must use the `diagnose debug application ospfd` to set the debugging level to 8 or higher. To configure OSPF routing, see config router ospf on page 26.

Use these commands to manage OSPF debugging:

```
diagnose ip router ospf cpu-usage show
diagnose ip router ospf crash-backtrace {clear | read}
```

```
diagnose ip router ospf debug all {enable | disable}
diagnose ip router ospf debug event {enable | disable}
diagnose ip router ospf debug ism {enable | disable}
diagnose ip router ospf debug lsa {enable | disable}
diagnose ip router ospf debug nsm {enable | disable}
diagnose ip router ospf debug nssa {enable | disable}
diagnose ip router ospf debug packet {enable | disable}
diagnose ip router ospf debug show
diagnose ip router ospf debug zebra {enable | disable}
diagnose ip router ospf ism-debug all {enable | disable}
diagnose ip router ospf ism-debug events {enable | disable}
diagnose ip router ospf ism-debug status {enable | disable}
diagnose ip router ospf ism-debug timers {enable | disable}
diagnose ip router ospf lsa-debug all {enable | disable}
diagnose ip router ospf lsa-debug flooding {enable | disable}
diagnose ip router ospf lsa-debug generate {enable | disable}
diagnose ip router ospf lsa-debug install {enable | disable}
diagnose ip router ospf lsa-debug refresh {enable | disable}
diagnose ip router ospf memory-usage show
diagnose ip router ospf nsm-debug all {enable | disable}
diagnose ip router ospf nsm-debug events {enable | disable}
diagnose ip router ospf nsm-debug status {enable | disable}
diagnose ip router ospf nsm-debug timers {enable | disable}
diagnose ip router ospf packet-debug all {enable | disable}
diagnose ip router ospf packet-debug dd {enable | disable}
diagnose ip router ospf packet-debug hello {enable | disable}
diagnose ip router ospf packet-debug ls-ack {enable | disable}
diagnose ip router ospf packet-debug ls-request {enable | disable}
diagnose ip router ospf packet-debug ls-update {enable | disable}
diagnose ip router ospf work-queues show
diagnose ip router ospf zebra-debug all {enable | disable}
diagnose ip router ospf zebra-debug interface {enable | disable}
diagnose ip router ospf zebra-debug redistribute {enable | disable}
```

Variable	Description
cpu-usage show	Display statistics for CPU usage.
crash-backtrace {clear | read}	Erase or display the OSPF crash backtrace information.
debug all {enable | disable}	Enable or disable all OSPF debugging.
debug event {enable | disable}	Enable or disable OSPF event debugging.
debug ism {enable | disable}	Enable or disable OSPF interface state machine (ISM) debugging.
debug lsa {enable | disable}	Enable or disable OSPF link state advertisement (LSA) debugging.
debug nsm {enable | disable}	Enable or disable OSPF neighbor state machine (NSM) debugging.
debug nssa {enable | disable}	Enable or disable OSPF Not So Stubby areas (NSSA) debugging.
debug packet {enable | disable}	Enable or disable OSPF packet debugging.

Variable	Description
debug show	Display the OSPF debugging level and which kinds of OSPF debugging are enabled.
debug zebra {enable | disable}	Enable or disable communication with the core router daemon.
ism-debug all {enable | disable}	Enable or disable all OSPF ISM debugging.
ism-debug events {enable | disable}	Enable or disable OSPF ISM event debugging.
ism-debug status {enable | disable}	Enable or disable OSPF ISM status debugging.
ism-debug timers {enable | disable}	Enable or disable OSPF ISM timers debugging.
lsa-debug all {enable | disable}	Enable or disable all OSPF LSA debugging.
lsa-debug flooding {enable | disable}	Enable or disable OSPF LSA flooding debugging.
lsa-debug generate {enable | disable}	Enable or disable OSPF LSA generation debugging.
lsa-debug install {enable | disable}	Enable or disable OSPF LSA installation and removal debugging.
lsa-debug refresh {enable | disable}	Enable or disable OSPF LSA refresh debugging.
memory-usage show	Display statistics for memory usage.
nsm-debug all {enable | disable}	Enable or disable all OSPF NSM debugging.
nsm-debug events {enable | disable}	Enable or disable OSPF NSM event debugging.
nsm-debug status {enable | disable}	Enable or disable OSPF NSM status debugging.
nsm-debug timers {enable | disable}	Enable or disable OSPF NSM timers debugging.
packet-debug all {enable | disable}	Enable or disable all OSPF packet debugging.
packet-debug dd {enable | disable}	Enable or disable database description packet debugging.
packet-debug hello {enable | disable}	Enable or disable hello packet debugging.
packet-debug ls-ack {enable | disable}	Enable or disable link state acknowledgment packet debugging.
packet-debug ls-request {enable | disable}	Enable or disable link state request packet debugging.

Variable	Description
packet-debug ls-update {enable | disable}	Enable or disable link statue update packet debugging.
work-queues show	Display information about work queues.
zebra-debug all {enable | disable}	Enable or disable all OSPF core router debugging.
zebra-debug interface {enable | disable}	Enable or disable OSPF core router interface debugging.
zebra-debug redistribute {enable | disable}	Enable or disable OSPF core router redistribution debugging.

Example output

```
S524DF4K15000024 # diagnose ip router ospf cpu-usage show
                      CPU (user+system): Real (wall-clock):
Runtime(ms)   Invoked Avg uSec Max uSecs Avg uSec Max uSecs  Type  Thread
0.000         1       0        0        130       130      E   zclient_connect
0.000      1332       0        0        23        90       T   ospf_lsa_refresh_
walker
0.000         1       0        0        145       145      T   ospf_spf_calculate_
timer
0.000         1       0        0        56        56       T   ospf_abr_task_timer
10.001        98      102      10001    124       6396 R       zclient_read
0.000       444       0        0        27        36       T   ospf_lsa_maxage_
walker
0.000       393       0        0        130       10301  W     vty_flush
150.011       392     382      10001      369     10470 R       vty_read
0.000         1       0        0        41        41       T   ospf_ase_calculate_
timer
0.000         6       0        0        101       211 R        vty_accept
0.000         1       0        0        36        36       T   (ospf_maxage_lsa_
remover)
160.012      2670       59     10001       94     10470 RWTEXB TOTAL

S524DF4K15000024 # diagnose ip router ospf memory-usage show
System allocator statistics:
Total heap allocated:  396 KiB
Holding block headers: 0 bytes
Used small blocks:     0 bytes
Used ordinary blocks:  385 KiB
Free small blocks:     64 bytes
Free ordinary blocks:  11 KiB
Ordinary blocks:       5
Small blocks:          4
Holding blocks:        0
(see system documentation for 'mallinfo' for meaning)
-----------------------------
Temporary memory             :          4
```

```
String vector                 :          3
Vector                        :        839
Vector index                  :        839
Link List                     :        179
Link Node                     :        182
Thread                        :         11
Thread master                 :          1
Thread stats                  :         11
VTY                           :          2
VTY history                   :          1
Interface                     :         76
Connected                     :         14
Buffer                        :          2
Buffer data                   :          1
Stream                        :          3
Stream data                   :          3
Prefix                        :         19
Hash                          :          1
Hash Bucket                   :         11
Hash Index                    :          1
Route table                   :        185
Route node                    :         34
Access List                   :          3
Access List Str               :          3
Access Filter                 :          3
Prefix List                   :          2
Prefix List Entry             :          2
Prefix List Str               :          2
Command desc                  :       8858
Logging                       :          1
Zclient                       :          1
Priority queue                :          2
Priority queue data           :          2
Host config                   :          4
----------------------------
OSPF top                      :          1
OSPF area                     :          1
OSPF LSA                      :          7
OSPF LSA data                 :          7
OSPF LSDB                     :          2
OSPF ext. info                :          6
OSPF if info                  :         76
OSPF if params                :         76
----------------------------
```

diagnose ip router rip

NOTE: To enable RIP debugging, you must use the `diagnose debug application ripd` to set the debugging level to 8 or higher. To configure RIP routeing, see "config router" on page 34.

Use these commands to manage RIP debugging:

```
diagnose ip router rip cpu-usage show
diagnose ip router rip crash-backtrace {clear | read}
diagnose ip router rip debug all {enable | disable}
diagnose ip router rip debug events {enable | disable}
diagnose ip router rip debug packet-rx {enable | disable}
diagnose ip router rip debug packet-tx {enable | disable}
diagnose ip router rip debug show
diagnose ip router rip debug zebra {enable | disable}
diagnose ip router rip memory-usage show
diagnose ip router rip work-queues show
```

Variable	Description
cpu-usage show	Display statistics for CPU usage.
crash-backtrace {clear | read}	Erase or display the RIP crash backtrace information.
debug all {enable | disable}	Enable or disable all RIP debugging.
debug events {enable | disable}	Enable or disable RIP event debugging.
debug packet-rx {enable | disable}	Enable or disable received RIP packet debugging.
debug packet-tx {enable | disable}	Enable or disable transmitted RIP packet debugging.
debug show	Display the RIP debugging level and which kinds of RIP debugging are enabled.
debug zebra {enable | disable}	Enable or disable communication with the core router daemon.
memory-usage show	Display statistics for memory usage.
work-queues show	Display information about work queues.

Example output

```
S524DF4K15000024 # diagnose ip router rip cpu-usage show
CPU (user+system): Real (wall-clock):
Runtime(ms)   Invoked Avg uSec Max uSecs Avg uSec Max uSecs  Type  Thread
0.000      2947        0          0      350        463    T    rip_update
0.000         1        0          0      685        685     E   zclient_connect
0.000      5904        0          0       13         76 R       rip_read
10.000       95      105      10000      260      17090 R       zclient_read
10.001      134       74      10001      170       9266  W      vty_flush
0.000         2        0          0      202        287    T    rip_interface_wakeup
0.000         5        0          0      158        407    T    rip_triggered_inter-
val
30.002      133      225      10001      364      10672 R       vty_read
0.000         3        0          0      227        314     E   rip_triggered_update
0.000         7        0          0       87        167 R       vty_accept
50.003     9231        5      10001      131      17090 RWTEXB TOTAL
```

```
S524DF4K15000024 # diagnose ip router rip memory-usage show
System allocator statistics:
Total heap allocated:  264 KiB
Holding block headers: 0 bytes
Used small blocks:     0 bytes
Used ordinary blocks:  228 KiB
Free small blocks:     1608 bytes
Free ordinary blocks:  36 KiB
Ordinary blocks:       4
Small blocks:          98
Holding blocks:        0
(see system documentation for 'mallinfo' for meaning)
-----------------------------
Temporary memory              :          1
String vector                 :          3
Vector                        :        587
Vector index                  :        587
Link List                     :         85
Link Node                     :         96
Thread                        :         11
Thread master                 :          1
Thread stats                  :         10
VTY                           :          2
VTY history                   :          1
Interface                     :         76
Connected                     :         14
Buffer                        :          2
Buffer data                   :          1
Stream                        :          3
Stream data                   :          3
Prefix                        :         19
Hash                          :          3
Hash Bucket                   :         10
Hash Index                    :          3
Route table                   :          5
Route node                    :          9
Access List                   :          3
Access List Str               :          3
Access Filter                 :          3
Prefix List                   :          2
Prefix List Entry             :          2
Prefix List Str               :          2
Route map                     :          1
Route map name                :          1
Route map index               :          1
Route map rule                :          4
Route map rule str            :          4
Route map compiled            :          4
Command desc                  :       6441
Key                           :          1
Key chain                     :          1
```

```
Logging                       :          1
Zclient                       :          1
Priority queue                :          2
Priority queue data           :          2
Host config                   :          4
-----------------------------
RIP structure                 :          1
RIP route info                :          4
RIP interface                 :         76
-----------------------------
```

diagnose ip router terminal monitor

Use this command to enable or disable the display of router information on the terminal:

```
diagnose ip router terminal monitor {enable | disable}
```

diagnose ip router zebra

NOTE: To enable debugging of the core router daemon, you must use the `diagnose debug application zebra` to set the debugging level to 8 or higher.

Use these commands to manage the core router daemon:

```
diagnose ip router zebra cpu-usage show
diagnose ip router zebra crash-backtrace {clear | read}
diagnose ip router zebra debug all {enable | disable}
diagnose ip router zebra debug events {enable | disable}
diagnose ip router zebra debug fpm {enable | disable}
diagnose ip router zebra debug kernel {enable | disable}
diagnose ip router zebra debug packet-rx {enable | disable}
diagnose ip router zebra debug packet-rx-detail {enable | disable}
diagnose ip router zebra debug packet-tx {enable | disable}
diagnose ip router zebra debug packet-tx-detail {enable | disable}
diagnose ip router zebra debug rib {enable | disable}
diagnose ip router zebra debug rib-queue {enable | disable}
diagnose ip router zebra debug show
diagnose ip router zebra fpm-counters {clear | show}
diagnose ip router zebra memory-usage show
diagnose ip router zebra work-queues show
```

Variable	Description
cpu-usage show	Display statistics for CPU usage.
crash-backtrace {clear | read}	Erase or display the crash backtrace information for the core router daemon.
debug all {enable | disable}	Enable or disable all debugging for the core router daemon.

Variable	Description
debug events {enable | disable}	Enable or disable event debugging for the core router daemon.
debug fpm {enable | disable}	Enable or disable hardware offload debugging for the core router daemon.
debug kernel {enable | disable}	Enable or disabe kernel interaction debugging for the core router daemon.
debug packet-rx {enable | disable}	Enable or disable general debugging of received packets for the core router daemon.
debug packet-rx-detail {enable | disable}	Enable or disable detailed debugging of received packets for the core router daemon.
packet-tx {enable | disable}	Enable or disable general debugging of transmitted packets for the core router daemon.
debug packet-tx-detail {enable | disable}	Enable or disable detailed debugging of transmitted packets for the core router daemon.
debug rib {enable | disable}	Enable or disable routing table debugging for the core router daemon.
debug rib-queue {enable | disable}	Enable or disable routing queue debugging for the core router daemon.
debug show	Display the debugging level of the core router daemon and which kinds of debugging of the core router daemon are enabled.
fpm-counters {clear | show}	Erase or display the hardware offload counters.
memory-usage show	Display statistics for memory usage.
work-queues show	Display information about work queues.

Example output

```
S524DF4K15000024 # diagnose ip router zebra cpu-usage show
CPU (user+system): Real (wall-clock):
Runtime(ms)   Invoked Avg uSec Max uSecs Avg uSec Max uSecs  Type  Thread
0.000         38         0          0        55       1042       B work_queue_run
0.000          4         0          0        63         73 R       zebra_accept
0.000          7         0          0        48        119 R       zfpm_read_cb
0.000          1         0          0       299        299   T     zfpm_connect_cb
0.000         92         0          0       158       5277  W      vty_flush
0.000       9167         0          0        15         26   T     zfpm_stats_timer_cb
10.001        28       357      10001       924      24068 R       zebra_client_read
10.001        91       109      10001       202        914 R       vty_read
10.000        98       102      10000        43        173 R       kernel_read
0.000          1         0          0        34         34       B zfpm_conn_up_thread_
cb
0.000         16         0          0        67        142  W      zfpm_write_cb
```

```
10.001        11      909     10001      107       234 R      vty_accept
40.003      9554        4     10001       22     24068 RWTEXB TOTAL

S524DF4K15000024 # diagnose ip router zebra fpm-counters show

Counter                                         Total     Last 10 secs

connect_calls                                       1                0
connect_no_sock                                     0                0
read_cb_calls                                       7                0
write_cb_calls                                     16                0
write_calls                                        13                0
partial_writes                                      0                0
max_writes_hit                                      0                0
t_write_yields                                      0                0
nop_deletes_skipped                                 8                0
route_adds                                         13                0
route_dels                                          0                0
updates_triggered                                  21                0
non_fpm_table_triggers                              0                0
redundant_triggers                                  5                0
dests_del_after_update                              0                0
t_conn_down_starts                                  0                0
t_conn_down_dests_processed                         0                0
t_conn_down_yields                                  0                0
t_conn_down_finishes                                0                0
t_conn_up_starts                                    1                0
t_conn_up_dests_processed                           8                0
t_conn_up_yields                                    0                0
t_conn_up_aborts                                    0                0
t_conn_up_finishes                                  1                0

S524DF4K15000024 # diagnose ip router zebra memory-usage show
System allocator statistics:
Total heap allocated:  396 KiB
Holding block headers: 0 bytes
Used small blocks:     0 bytes
Used ordinary blocks:  295 KiB
Free small blocks:     2384 bytes
Free ordinary blocks:  101 KiB
Ordinary blocks:       3
Small blocks:          148
Holding blocks:        0
(see system documentation for 'mallinfo' for meaning)
-----------------------------
Temporary memory              :         78
String vector                 :          3
Vector                        :        691
Vector index                  :        691
Link List                     :        169
Link Node                     :        109
Thread                        :         16
```

```
Thread master                  :          1
Thread stats                   :         12
VTY                            :          2
VTY history                    :          1
Interface                      :         76
Connected                      :         14
Buffer                         :          5
Buffer data                    :          1
Stream                         :         10
Stream data                    :         10
Prefix                         :         19
Hash                           :          1
Hash Bucket                    :         12
Hash Index                     :          1
Route table                    :         86
Route node                     :         45
Access List                    :          3
Access List Str                :          3
Access Filter                  :          3
Prefix List                    :          2
Prefix List Entry              :          2
Prefix List Str                :          2
Route map name                 :          2
Command desc                   :       7201
Logging                        :          1
Work queue                     :          2
Work queue name string         :          1
Priority queue                 :          2
Priority queue data            :          2
Host config                    :          4
----------------------------
VRF                            :          1
VRF name                       :          1
Nexthop                        :         25
RIB                            :         25
Static IPv4 route              :          2
RIB destination                :         19
RIB table info                 :          4
----------------------------
BFD candidate table            :          1
----------------------------

S524DF4K15000024 # diagnose ip router zebra work-queues show
List (ms)   Q. Runs       Cycle Counts
P    Items  Hold    Total    Best  Gran.   Avg. Name
0    10       38       1      1      1 route_node processing
```

diagnose ip rtcache list

Use this command to list the routing cache:

```
diagnose ip rtcache list
```

diagnose ip tcp

Use this command to list or clear the TCP sockets:

```
diagnose ip tcp {list | flush}
```

Example

```
S524DF4K15000024 # diagnose ip tcp list

sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid
timeout inode
0: 00000000:03E8 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0
   0 3099 1 e647d300 100 0 0 10 -1
1: 00000000:0A29 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0
   0 1587 1 e647c000 100 0 0 10 -1
2: 00000000:0A2A 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0
   0 3338 1 e647dc80 100 0 0 10 -1
3: 00000000:03EB 00000000:0000 0A 00000000:00000000 00:00000000 00000000     0
   0 3103 1 e647d7c0 100 0 0 10 -1
...
```

diagnose ip udp

Use this command to list or clear the UDP sockets:

```
diagnose ip udp {list | flush}
```

Example

```
S524DF4K15000024 # diagnose ip udp list
sl  local_address rem_address   st tx_queue rx_queue tr tm->when retrnsmt   uid
timeout inode ref pointer drops
24: 00000000:E818 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
    0 4097 2 e69e38c0 0
53: 00000000:0035 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
    0 1972 2 e6029440 0
67: 00000000:0043 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
    0 964 2 e5fd2d80 0
67: 00000000:0043 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
    0 963 2 e5fd2b40 0
68: 00000000:0044 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
    0 1961 2 e6029200 0
181: 00000000:90B5 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 7681206 2 e6b94b40 0
350: 00000000:C15E 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3301 2 e69e2b40 0
370: 0100007F:1972 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 1793 2 e6028fc0 0
404: 00000000:B994 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 112 2 e5fd2000 0
```

```
415: 00000000:859F 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 11905 2 e5fd38c0 0
415: 00000000:C99F 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3113 2 e6029d40 0
450: 00000000:E9C2 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 157 2 e5fd2480 0
520: 00000000:0208 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 2196 2 e5fd3680 0
546: 00000000:CA22 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 2156 2 e5fd3440 0
549: 00000000:9225 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 2057 2 e5fd2fc0 0
653: 00000000:AE8D 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 775 2 e5fd2900 0
654: 00000000:B68E 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 1977 2 e6029b00 0
688: 00000000:12B0 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3321 2 e69e2fc0 0
712: 00000000:0EC8 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3320 2 e69e2d80 0
713: 00000000:0EC9 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3322 2 e69e3200 0
763: 00000000:92FB 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 9848617 2 e6ad7200 0
788: 0100007F:0714 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3224 2 e69e2240 0
805: 0100007F:A725 0100007F:0714 01 00000000:00000000 00:00000000 00000000     0
     0 3292 2 e69e2900 0
882: 00000000:8372 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 1974 2 e60298c0 0
972: 00000000:B7CC 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 3260 2 e69e26c0 0
981: 00000000:EBD5 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 39752 2 e69e3b00 0
990: 00000000:BBDE 00000000:0000 07 00000000:00000000 00:00000000 00000000     0
     0 4357 2 e69e3d40 0
```

diagnose ipv6 address

Use these commands to manage IPv6 addresses:

```
diagnose ipv6 address add <interface_name> <IPv6_address>
diagnose ipv6 address anycast <arguments>
diagnose ipv6 address delete <interface_name> <IPv6_address>
diagnose ipv6 address flush
diagnose ipv6 address list
diagnose ipv6 address multicast <interface_name> <IPv6_address>
```

Variable	Description
add <interface_name> <IPv6_address>	Add an IPv6 address to the specified interface. Use the following format for the IPv6 address: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx
anycast <arguments>	Add an IPv6 anycast address.
delete <interface_name> <IPv4_address>	Delete an IPv6 address from the specified interface. Use the following format for the IPv6 address: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx
flush	Delete all IPv6 addresses.
list	List all IPv6 addresses and which interfaces they are assigned to.
multicast <interface_name> <IPv6_address>	Add an IPv6 multicast address to the specified interface. Use the following format for the IPv6 address: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx

Example output

```
S524DF4K15000024 # diagnose ipv6 address list

dev=1 devname=lo flag=P scope=254 prefix=128 addr=::1 prefered=-1 valid=-1
dev=2 devname=mgmt flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fef1:95e4 pref-
ered=-1 valid=-1
dev=70 devname=internal flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fef1:95e5
prefered=-1 valid=-1
dev=71 devname=vlan35 flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fef1:95e5 pref-
ered=-1 valid=-1
dev=72 devname=vlan85 flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fef1:95e5 pref-
ered=-1 valid=-1
dev=74 devname=vlan-8 flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fef1:95e5 pref-
ered=-1 valid=-1
```

diagnose ipv6 devconf

Use these commands to configure IPv6 devices:

```
diagnose ipv6 address devconf accept-dad {0 | 1 | 2}
diagnose ipv6 address devconf disable_ipv6 {0 | 1 }
```

Variable	Description
accept-dad {0 | 1 | 2}	Configure the detection of duplicate IPv6 address: • 0 — disable duplicate address detection. • 1 — enable duplicate address detection. • 2 — enable duplicate address detection and disable IPv6 operation if duplicate MAC-based link-local addresses are found.
disable_ipv6 {0 | 1 }	Configure IPv6 operation: • 0 — enable IPv6 operation. • 1 — disableIPv6 operation.

diagnose ipv6 ipv6-tunnel

Use these commands to manage IPv6 tunnels:

```
diagnose ipv6 ipv6-tunnel add <tunnel_name> <interface_name> <source_IPv6_address>
    <destination_IPv6_address>
diagnose ipv6 ipv6-tunnel delete <tunnel_name>
diagnose ipv6 ipv6-tunnel list
```

Variable	Description
add <tunnel_name> <interface_name> <source_IPv6_address> <destination_IPv6_address>	Create a tunnel between two IPv6 addresses on the specified interface. Use the following format for the IPv6 addresses: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
delete <tunnel_name>	Delete the specified IPv6 tunnel.
delete <interface_name> <IPv4_address>	List all IPv6 tunnels.

Example output

```
S524DF4K15000024 # diagnose ipv6 ipv6-tunnel list

sys_list_tunnel6:233 not implemented
```

diagnose ipv6 neighbor-cache

Use these commands to manage the IPv6 Address Resolution Protocol (ARP) table:

```
diagnose ipv6 neighbor-cache add <interface_name> <IPv6_address> <MAC_address>
diagnose ipv6 neighbor-cache delete <interface_name> <IPv4_address>
diagnose ipv6 neighbor-cache flush <interface_name>
diagnose ipv6 neighbor-cache list
```

Variable	Description
add <interface_name> <IPv6_address>	Add an ARP entry for the IPv6 address on the specified interface.
delete <interface_name> <IPv6_address>	Delete an ARP entry for the IPv6 address on the specified interface.
flush <interface_name>	Delete the ARP table for the specified interface.
list	Display the ARP table.

Example output

```
S524DF4K15000024 # diagnose ipv6 neighbor-cache list

ifindex=1 ifname=lo :: 00:00:00:00:00:00 state=00000040 use=1096280 con-
firm=1102281 update=1096280 ref=6
```

diagnose ipv6 route

Use these commands to manage the IPv6 routing table:

```
diagnose ipv6 route flush
diagnose ipv6 route list
```

Variable	Description
flush	Delete the routing table.
list	Display the routing table.

Example output

```
S524DF4K15000024 # diagnose ipv6 route list

type=02 protocol=unspec flag=00000000 oif=1(lo) dst:::1/128 gwy::: prio=0
type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::a5b:eff:fef1:95e4/128
gwy::: prio=0
type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::a5b:eff:fef1:95e5/128
gwy::: prio=0
type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::a5b:eff:fef1:95e5/128
gwy::: prio=0
type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::a5b:eff:fef1:95e5/128
gwy::: prio=0
type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::a5b:eff:fef1:95e5/128
gwy::: prio=0
type=01 protocol=kernel flag=00000000 oif=70(internal) dst:fe80::/64 prio=100
type=01 protocol=kernel flag=00000000 oif=74(vlan-8) dst:fe80::/64 prio=100
type=01 protocol=kernel flag=00000000 oif=71(vlan35) dst:fe80::/64 prio=100
```

```
type=01 protocol=kernel flag=00000000 oif=72(vlan85) dst:fe80::/64 prio=100
type=01 protocol=kernel flag=00000000 oif=2(mgmt) dst:fe80::/64 prio=100
type=01 protocol=boot flag=00000000 oif=70(internal) dst:ff00::/8 prio=100
type=01 protocol=boot flag=00000000 oif=74(vlan-8) dst:ff00::/8 prio=100
type=01 protocol=boot flag=00000000 oif=71(vlan35) dst:ff00::/8 prio=100
type=01 protocol=boot flag=00000000 oif=72(vlan85) dst:ff00::/8 prio=100
type=01 protocol=boot flag=00000000 oif=2(mgmt) dst:ff00::/8 prio=100
type=07 protocol=kernel flag=00000000 oif=73(int1) prio=ffffffff
```

diagnose ipv6 sit-tunnel

Use these commands to manage IPv4 tunnels:

```
diagnose ipv6 sit-tunnel add <tunnel_name> <interface_name> <source_IPv4_address>
    <destination_IPv4_address>
diagnose ipv6 sit-tunnel delete <tunnel_name>
diagnose ipv6 sit-tunnel list
```

Variable	Description
add <tunnel_name> <interface_name> <source_IPv4_address> <destination_IPv4_address>	Create a tunnel between two IPv4 addresses on the specified interface. Use the following format for the IPv4 addresses: XXX.XXX.XXX.XXX
delete <tunnel_name>	Delete the specified IPv4 tunnel.
delete <interface_name> <IPv4_address>	List all IPv4 tunnels.

Example output

```
S524DF4K15000024 # diagnose ipv6 sit-tunnel list

sys_list_tunnel6:263 not implemented
```

diagnose log alertconsole

Use the following commands to manage alert console messages:

```
diagnose log alertconsole clear
diagnose log alertconsole fgd-retrieve
diagnose log alertconsole list
diagnose log alertconsole test
```

Variable	Description
clear	Clear alert console messages.

Variable	Description
fgd-retrieve	Retrieve FortiGuard alert console messages.
list	List current alert console messages.
test	Generate alert console messages.

Example output

```
S524DF4K15000024 # diagnose log alertconsole list

There are 50 alert console messages:
2017-10-10 13:26:07 Administrator acmin login failed
2017-10-09 15:41:32 Firmware upgraded by admin
2017-09-29 15:14:11 Firmware upgraded by admin
2017-09-28 07:45:38 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-09-28 07:45:35 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-09-28 07:45:32 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-09-26 08:46:09 Firmware upgraded by admin
2017-09-21 16:16:59 Firmware upgraded by admin
2017-09-19 15:21:16 Administrator [3~[3~[3~ login failed
2017-09-12 16:29:22 Administrator get test dnsproxy ? login failed
2017-09-11 15:49:17 Administrator get router prefix-list login failed
2017-09-06 08:37:44 Firmware upgraded by FortiCloud
2017-09-05 16:49:54 Administrator R  1 login failed
2017-09-01 07:30:03 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-09-01 07:30:00 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-09-01 07:29:57 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-08-31 16:56:35 Administrator O  1 login failed
2017-08-31 16:53:34 Administrator R u 1 login failed
2017-08-31 16:20:29 Administrator cinfcon login failed
2017-08-29 08:37:56 Firmware upgraded by FortiCloud
2017-08-25 13:26:49 Administrator sdmin login failed
2017-08-24 11:00:46 Administrator conconfig login failed
2017-08-24 08:29:01 Firmware upgraded by FortiCloud
2017-08-21 09:16:13 Firmware upgraded by unknown
2017-08-21 08:58:20 System shutdown (factory default)
2017-08-16 08:31:31 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-08-16 08:31:28 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-08-16 08:31:25 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-08-15 07:33:29 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
2017-08-15 07:33:26 Administrator ERROR: Class:0; Subclass:10000; Ope login failed
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
```

```
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
1969-12-31 17:00:07 System restart
```

diagnose log-stats show

Use this command to retrieve logging statistics:

```
diagnose log-stats show
```

diagnose loop-guard instance status

Use this command to display which ports have loop guard enabled:

```
diagnose loop-guard instance status
```

To enable loop guard on a port, see config switch interface on page 54.

Example output

```
S524DF4K15000024 # diagnose loop-guard instance status

Portname              State      Status       Timeout(m)     Count    Last-Event
__________________   _______    _________    ___________    _____   _______________

port1               disabled     -              -             -           -
port2               disabled     -              -             -           -
port3               disabled     -              -             -           -
port4               disabled     -              -             -           -
port5               disabled     -              -             -           -
port6               disabled     -              -             -           -
port9               disabled     -              -             -           -
port10              enabled      -              45            0           -
port11              disabled     -              -             -           -
port12              disabled     -              -             -           -
port13              disabled     -              -             -           -
port14              disabled     -              -             -           -
port15              disabled     -              -             -           -
port16              disabled     -              -             -           -
port17              disabled     -              -             -           -
port18              disabled     -              -             -           -
port19              disabled     -              -             -           -
port20              enabled      -              45            0           -
port21              disabled     -              -             -           -
```

```
port22              disabled     -              -              -              -
port23              disabled     -              -              -              -
port24              disabled     -              -              -              -
port25              disabled     -              -              -              -
port26              disabled     -              -              -              -
port27              disabled     -              -              -              -
port28              disabled     -              -              -              -
port29              disabled     -              -              -              -
port30              enabled      -              45             0              -
```

diagnose properties

Use these commands to manage property values:

```
diagnose properties get <property>
diagnose properties set <property> <value>
diagnose properties unset <property>
```

Variable	Description
get <property>	Display the value of a property.
set <property> <value>	Specify the value of a property.
unset <property>	Delete a property.

Example

This example sets the value of the `key1` property and then displays it:

```
S524DF4K15000024 # diagnose properties set key1 5

S524DF4K15000024 # diagnose properties get key1

5
```

diagnose settings

Use these commands to manage diagnostic settings:

```
diagnose settings info
diagnose settings reset
```

Variable	Description
info	List all diagnostic settings.
reset	Reset all diagnostic settings to their default settings.

Example output

```
S524DF4K15000024 # diagnose settings info

debug output:           disable
console timestamp:      disable
console no user log message:    disable
fsmgr debug level:      16 (0x10)
CLI debug level:        3
```

diagnose sniffer packet

Use this command to examine packets received on a specific interface:

```
diagnose sniffer packet <interface_name | any> <logical_filter | none> <verbose | 1-6>
    <sniffer_count> <timestamp_format>
```

Variable	Description
<interface_name | any>	Enter the name of a network interface or enter `any` to examine packets received on all interfaces.

<logical_filter | none>	Enter a logical filter or `none`. Use the following format for the filter:
	`'[[src|dst] host<IP_address>] [[src|dst] host<IP_address>] [[arp|ip|gre|esp|udp|tcp] [port_number]] [[arp|ip|gre|esp|udp|tcp] [port_number]]'`
	
	For example, to examine UDP packets received at port 1812 from host forti1 and host forti2 or forti3:
	`'udp and port 1812 and host forti1 and \( forti2 or forti3 \)'`
	
	To examine TCP packets between two PCs through port 80:
	`diag sniffer packet internal 'host 192.168.0.130 and 192.168.0.1 and tcp port 80' 1`
	
	To examine packets with the RST flag set:
	`diagnose sniffer packet internal "tcp[13] & 4 != 0"`
	
	To examine packets with the destination MAC address of 00:09:0f:89:10:ea:
	`diagnose sniffer packet internal "(ether [0:4]=0x00090f89) and (ether[4:2]=0x10ea)"`

Variable	Description
<verbose | 1-6>	Set the level of detail for the results: • `verbose` — Display all details. • `1` — Include the packet header. • `2` — Include the packet header and IP address data. • `3` — Include the packet header and Ethernet address data (if available). • `4`— Include the packet header and interface name. • `5` — Include the packet header, interface name, and IP address data. • `6` — Include the packet header, interface name, and Ethernet address data (if available).
<sniffer_count>	Enter the number of packets to examine.
<timestamp_format>	Enter `a` for UTC time (`yyyy-mm-dd hh:mm:ss.ms`) or enter the number of minutes and seconds after the start of the packet examination (`ss.ms`).

Example output

```
S524DF4K15000024 # diagnose sniffer packet any
interfaces=[any]
filters=[none]
0.977537 arp who-has 192.168.0.10 tell 192.168.1.99
0.977755 127.0.0.1 -> 0.0.0.0: icmp: type-#20
1.057565 224.0.0.18 -> 33.5.255.1:  ip-proto-10 (frag 65392:4294967276@1336+)
1.057578 802.1Q vlan#8 P0 -- 224.0.0.18 -> 33.5.255.1:  ip-proto-10 (frag
65392:4294967276@1336+)
1.113131 arp who-has 10.105.16.1 tell 10.105.19.8
1.977047 arp who-has 192.168.0.10 tell 192.168.1.99
1.990059 127.0.0.1 -> 0.0.0.0: icmp: type-#20
...

S524DF4K15000024 # diagnose sniffer packet internal none verbose
interfaces=[internal]
filters=[none]
pcap_lookupnet: internal: no IPv4 address assigned
0.840645 802.1Q vlan#8 P0 -- 10.10.10.1 -> 224.0.0.18:  ip-proto-112 20
1.113149 arp who-has 192.168.0.10 tell 192.168.1.99
1.850162 802.1Q vlan#8 P0 -- 10.10.10.1 -> 224.0.0.18:  ip-proto-112 20
2.109899 arp who-has 192.168.0.10 tell 192.168.1.99
2.859653 802.1Q vlan#8 P0 -- 10.10.10.1 -> 224.0.0.18:  ip-proto-112 20
3.109412 arp who-has 192.168.0.10 tell 192.168.1.99
3.869169 802.1Q vlan#8 P0 -- 10.10.10.1 -> 224.0.0.18:  ip-proto-112 20
4.128948 arp who-has 192.168.0.10 tell 192.168.1.99
...

S524DF4K15000024 # diagnose sniffer packet internal none 3 10 a
interfaces=[internal]
```

```
filters=[none]
pcap_lookupnet: internal: no IPv4 address assigned
2017-10-11 16:09:42.393816 arp who-has 192.168.0.10 tell 192.168.1.99
0x0000   ffff ffff ffff 085b 0ef1 95e5 0806 0001        .......[........
0x0010   0800 0604 0001 085b 0ef1 95e5 c0a8 0163        .......[.......c
0x0020   0000 0000 0000 c0a8 000a                       ..........

2017-10-11 16:09:42.483785 802.1Q vlan#8 P0 -- 10.10.10.1 -> 224.0.0.18:  ip-
proto-112 20
0x0000   0100 5e00 0012 0000 5e00 0105 8100 0008        ..^.....^.......
0x0010   0800 45c0 0028 8fec 0000 ff70 369c 0a0a        ..E..(.....p6...
0x0020   0a01 e000 0012 2105 ff01 0001 d392 0b01        ......!.........
0x0030   0164 0000 0000 0000 0000                       .d........
...
```

diagnose snmp

Use these commands to display SNMP information:

```
diagnose snmp ip frags
diagnose snmp trap send
```

Variable	Description
ip frags	Display fragmentation and reassembly information
trap send	Generate a trap event and send it to the SNMP daemon.

Example output

```
S524DF4K15000024 # diagnose snmp ip frags

ReasmTimeout = 0
ReasmReqds   = 0
ReasmOKs     = 0
ReasmFails   = 0
FragOKs      = 0
FragFails    = 0
FragCreates  = 0
```

diagnose stp instance list

Use this command to display information about Multiple Spanning Tree Protocol (MSTP) instances:

```
diagnose stp instance list <STP_ID> <port_number>
```

To create an STP instance, see config switch stp instance on page 75.

Variable	Description
<STP_ID>	Enter the STP identifier (0-15). If you enter a higher number than 15, results for all STP instances are displayed.
<port_number>	Enter the port number. If no port number is specified, results for all physical ports are displayed.

Example output

```
S524DF4K15000024 # diagnose stp instance list 16 port1

MST Instance Information, primary-Channel:

Instance ID :   0

Switch Priority : 32768

Root MAC Address :    085b0ef195e4
Root Priority:    32768
Root Pathcost:    0
Regional Root MAC Address :   085b0ef195e4
Regional Root Priority:   32768
Regional Root Path Cost:  0
Remaining Hops:       20
This Bridge MAC Address :    085b0ef195e4
This bridge is the root

Port               Speed   Cost       Priority   Role         State       Edge
STP-Status  Loop Protection
_________________   ______  _________  _________  ___________  __________  ____  __
________  _________________

port1              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO

Instance ID :   1
Mapped VLANs :

Switch Priority : 8192

Regional Root MAC Address :   085b0ef195e4
Regional Root Priority:   8192
Regional Root Path Cost:  0
Remaining Hops:       20
This Bridge MAC Address :    085b0ef195e4
This bridge is the root

Port               Speed   Cost       Priority   Role         State       Edge
STP-Status  Loop Protection
_________________   ______  _________  _________  ___________  __________  ____  __
________  _________________
```

diagnose stp mst-config list

Use this command to display the MSTP configuration:

```
diagnose snmp mst-config list
```

To configure an MSTP instance, see config switch stp settings on page 76.

Example output

```
S524DF4K15000024 # diagnose stp mst-config list

MST Configuration Identification Information

Unit: primary
MST Configuration Name: region1
MST Configuration Revision: 1
MST Configuration Digest: ac36177f50283cd4b83821d8ab26de62

Instance ID      Mapped VLANs     Priority
____________________________________________________
       0                           32768
       1                            8192
```

diagnose stp vlan list

Use this command to display the MSTP information for a specific VLAN:

```
diagnose stp vlan list <VLAN_ID>
```

Variable	Description
<VLAN_ID>	Enter the VLAN identifier. The value range is 1-4095.

Example output

```
S524DF4K15000024 # diagnose stp vlan list 10

MST Instance Information, primary-Channel:

Instance ID :   0

Switch Priority : 32768

Root MAC Address :    085b0ef195e4
Root Priority:    32768
Root Pathcost:    0
Regional Root MAC Address :   085b0ef195e4
Regional Root Priority:   32768
Regional Root Path Cost:  0
```

```
Remaining Hops:       20
This Bridge MAC Address :    085b0ef195e4
This bridge is the root

Port               Speed   Cost       Priority   Role         State       Edge
STP-Status  Loop Protection
_________________  ______  _________  _________  ___________  __________  ____  __
________  _______________

port1              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port2              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port3              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port4              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port5              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port6              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port9              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port10             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port11             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port12             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port13             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port14             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port15             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port16             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port17             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port18             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port19             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port20             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port21             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port22             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port23             -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port24             -       200000000  128        DISABLED     DISCARDING   YES
```

```
ENABLED        NO
port25              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port26              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port27              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port28              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port29              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
port30              -       200000000  128        DISABLED     DISCARDING   YES
ENABLED        NO
internal            1G      20000      128        DESIGNATED   FORWARDING   YES
DISABLED       NO
```

diagnose switch 802-1x status

Use this command to display the status of a port using IEEE 802.1x authentication:

```
diagnose switch 802-1x status [<port_name>]
```

Variable	Description
[<port_name>]	Enter the port name. If the port is not specified, the status of all 802.1x-authenticated ports is returned.

To enable IEEE 802.1x authentication on a port, see config switch interface on page 54.

Example output

```
S524DF4K15000024 # diagnose switch 802-1x status

port1 : Mode: port-based (mac-by-pass enable)
Link: Link down
Port State: unauthorized (  )

port2 : Mode: mac-based (mac-by-pass disable)
Link: Link down
Port State: unauthorized (  )
```

diagnose switch acl counter

Use these commands to display information about access control lists (ACLs):

```
diagnose switch acl counter all
diagnose switch acl counter app <name>
diagnose switch acl counter id <policy_ID>
diagnose switch acl counter list-apps
```

Variable	Description
all	List all applications using ACL counters.
app <name>	List ACL counters for this application.
id <policy_ID>	List the ACL counter for this ACL policy identifier.
list-apps	List application names that use ACL counters.

Example output

```
S524DF4K15000024 # diagnose switch acl counter list-apps

Application              Policy ID Range
_____________________________________________

loop-gaurd                (2049-2049)
l3-arp-req                (2050-2050)
l3-arp-reply              (2051-2051)
dst-mac                   (2052-2052)
bfd-single-hop            (2053-2053)
bfd-multi-hop             (2054-2054)
ospf                      (2055-2055)
rip                       (2056-2056)
mclag                     (2057-2057)
mclag-l3-arp-req          (2058-2058)
mclag-l3-arp-reply        (2059-2059)
mclag-bfd-single-hop      (2060-2060)
mclag-bfd-multi-hop       (2061-2061)
mclag-ospf                (2062-2062)
mclag-rip                 (2063-2063)
fortilink                 (2064-2064)
fortilink-1               (2065-2065)
mclag-fortilink           (2066-2066)
mclag-icl                 (2067-2067)
mac-sa-mcast              (2068-2068)
forti-trunk               (2069-2069)
vwire                     (2304-2367)
vwire-acl                 (2368-133503)
dhcp-snooping             (133504-141695)
arp-snooping              (141696-145792)
access-vlan               (145793-149889)
network-monitor           (149890-149930)
```

diagnose switch arp-inspection stats clear

Use this command to delete dynamic ARP inspection statistics:

```
diagnose switch arp-inspection stats clear <VLAN_ID>
```

Variable	Description
<VLAN_ID>	Enter a single VLAN identifier or a range of VLAN identifiers separated by commas. For example: 1,3-4,6,7,9-100

To enable dynamic ARP inspection on a VLAN, see config switch vlan on page 81.

diagnose switch egress list

Use this command to display the port egress map:

```
diagnose switch egress list <port_name>
```

Variable	Description
<port_name>	Enter the port name.

Example output

```
S524DF4K15000024 # diagnose switch egress list port1

Switch Interface Egress Map, primary-Channel
Port Map: Name(Id):

port1(1)            port2(2)            port3(3)
port4(4)            port5(5)            port6(6)
port7(7)            port8(8)            port9(9)
port10(10)          port11(11)          port12(12)
port13(13)          port14(14)          port15(15)
port16(16)          port17(17)          port18(18)
port19(19)          port20(20)          port21(21)
port22(22)          port23(23)          port24(24)
port25(25)          port26(26)          port27(27)
port28(28)          port29(29)          port30(30)
internal(31)
cpu0(31)

Source Interface  Destination Ports
________________  ___________________________________
port1             1-6,9-31
```

diagnose switch ip-mac-binding entry

Use this command to display the counters for an IP-MAC binding entry:

```
diagnose switch ip-mac-binding entry <entry_ID>
```

Variable	Description
<entry_ID>	Enter an IP-MAC binding entry identifier.

To enable IP-MAC binding, see config switch global on page 50.

Example output

```
S524DF4K15000024 # diagnose switch ip-mac-binding entry 1

Binding Entry: 1
Binding IP: 1.20.168.172 255.255.255.255
Binding MAC: 00:21:CC:D2:76:72
Status: Enabled
Statistic:
Permit packets: 0x00
Drop packets: 0x00
------------------------------------------------------
```

diagnose switch mac-address

Use these commands to manage the MAC address table:

```
diagnose switch mac-address delete {all | entry <xx:xx:xx:xx:xx:xx>}
diagnose switch mac-address filter clear
diagnose switch mac-address filter flags <flag bit pattern>
diagnose switch mac-address filter port-id-map <port-ID list>
diagnose switch mac-address filter show
diagnose switch mac-address filter trunk-id-map <trunk-ID list>
diagnose switch mac-address filter vlan-map <VLAN_list>
diagnose switch mac-address list
diagnose switch mac-address switch-port-macs-db
```

Variable	Description
delete {all | entry <xx:xx:xx:xx:xx:xx>}	Delete all MAC address entries or a specific MAC address entry.
filter clear	Delete the filter for the MAC address table list.
filter flags <flag bit pattern>	Specify the flag bit pattern to match. Use this pattern to mask important bits. This value is hexadecimal.
filter port-id-map <port-ID list>	List the port identifiers to display MAC addresses for. Separate the port identifiers with commas. For example: 1,3,5-17,19
filter show	Display the filter for the MAC address table list.

Variable	Description
filter trunk-id-map <trunk-ID list>	List the trunk identifiers to display MAC addresses for. Separate the trunk identifiers with commas. For example: 1,2-4,77
filter vlan-map <VLAN_list>	List the VLAN identifiers to display MAC addresses for. Separate the VLAN identifiers with commans. For example: 1,2-4,77
list	List the MAC address entries.
switch-port-macs-db	List which MAC addresses are assigned to local ports.

Example output

```
S524DF4K15000024 # diagnose switch mac-address filter show

flag bit pattern: 0x00000000
flag bit Mask:    0x00000000
vlan map: 0-4095
port-id map: 1,64
trunk-id map: 0-127

S524DF4K15000024 # diagnose switch mac-address switch-port-macs-db

Total MACs : 30

MAC-1   : 08:5b:0e:f1:95:e6
MAC-2   : 08:5b:0e:f1:95:e8
MAC-3   : 08:5b:0e:f1:95:ea
MAC-4   : 08:5b:0e:f1:95:ec
MAC-5   : 08:5b:0e:f1:95:ee
MAC-6   : 08:5b:0e:f1:95:f0
MAC-7   : 08:5b:0e:f1:95:f2
MAC-8   : 08:5b:0e:f1:95:f4
MAC-9   : 08:5b:0e:f1:95:f6
MAC-10  : 08:5b:0e:f1:95:f8
MAC-11  : 08:5b:0e:f1:95:fa
MAC-12  : 08:5b:0e:f1:95:fc
MAC-13  : 08:5b:0e:f1:95:fe
MAC-14  : 08:5b:0e:f1:96:00
MAC-15  : 08:5b:0e:f1:96:02
MAC-16  : 08:5b:0e:f1:95:e7
MAC-17  : 08:5b:0e:f1:95:e9
MAC-18  : 08:5b:0e:f1:95:eb
MAC-19  : 08:5b:0e:f1:95:ed
MAC-20  : 08:5b:0e:f1:95:ef
MAC-21  : 08:5b:0e:f1:95:f1
MAC-22  : 08:5b:0e:f1:95:f3
MAC-23  : 08:5b:0e:f1:95:f5
MAC-24  : 08:5b:0e:f1:95:f7
MAC-25  : 08:5b:0e:f1:95:f9
MAC-26  : 08:5b:0e:f1:95:fb
```

```
MAC-27  : 08:5b:0e:f1:95:fd
MAC-28  : 08:5b:0e:f1:95:ff
MAC-29  : 08:5b:0e:f1:96:01
MAC-30  : 08:5b:0e:f1:96:03
```

diagnose switch mclag

Use these commands to manage information about MCLAGs:

```
diagnose switch mclag clear-stats {all | icl | mclag <trunk_name>}
diagnose switch mclag icl
diagnose switch mclag list <trunk_name>
```

Variable	Description
clear-stats {all | icl | mclag}	Delete statistics for all MCLAGs, delete MCLAG ICLs, or delete the statistics for the MCLAG with the specified trunk.
icl	List all inter-chassis links (ICLs).
list <trunk_name>	Display statistics for the MCLAG with the specified trunk.

To set up an MCLAG, see config switch trunk on page 77.

Example output

```
S524DF4K15000024 # diagnose switch mclag icl

MCLAG-ICL-trunk
       icl-ports             port15 port16
       egress-block-ports    none
       interface-mac         08:5b:0e:f1:95:e5
       lacp-serial-number    S524DF4K15000024
       peer-info             N/A
       keepalive interval    1
       keepalive timeout     30

Counters
```

diagnose switch modules

Use these commands to display information about physical layer (PHY) modules:

```
diagnose switch modules eeprom <physical_port_name>
diagnose switch modules state-machine <physical_port_name>
```

Variable	Description
eeprom	Display fragmentation and reassembly information
trap send	Generate a trap event and send it to the SNMP daemon.

Example output

```
S524DF4K15000024 # diagnose switch modules state-machine port10

DMI Status
---------------------------------
monitor_interval   10 minutes
next_monitor_in    0:44
dmi_trace          0
alarm_trap_enabled 0
num_ports          30
mod_pres           0x0000000000000000
mod_rxlos          0x0000000000000000
state_runs         62380
state_transitions  6

           Module Summary             |               |    Alarm - Warning Flags    |
                                  DMI |    Module     |Temp | Vcc |TxBia|TxPwr|RxPwr|
port | curr state | prev state | -IC | Type | State
|Hi|Lo|Hi|Lo|Hi|Lo|Hi|Lo|Hi|Lo|
-------------------------------------------------------------------------------------
 1 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 2 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 3 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 4 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 5 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 6 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 7 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 8 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
 9 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
10 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
11 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
12 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
13 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
14 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
15 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
16 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
17 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
18 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
19 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
20 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
21 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
22 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
23 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
24 | INVALID    | INVALID    | 0-0 | NONE |INVALID|..|..|..|..|..|..|..|..|..|
25 | EMPTY      | EMPTY      | 0-0 | NONE |EMPTY  |..|..|..|..|..|..|..|..|..|
```

```
26 | EMPTY       | EMPTY       | 0-0 | NONE |EMPTY   |..|..|..|..|..|..|..|..|..|..|
27 | EMPTY       | EMPTY       | 0-0 | NONE |EMPTY   |..|..|..|..|..|..|..|..|..|..|
28 | EMPTY       | EMPTY       | 0-0 | NONE |EMPTY   |..|..|..|..|..|..|..|..|..|..|
29 | EMPTY       | EMPTY       | 0-0 | NONE |EMPTY   |..|..|..|..|..|..|..|..|..|..|
30 | EMPTY       | EMPTY       | 0-0 | NONE |EMPTY   |..|..|..|..|..|..|..|..|..|..|
```

diagnose switch network-monitor

Use these commands to manage information produced by network monitoring:

```
diagnose switch network-monitor cfg-stats
diagnose switch network-monitor clear-db
diagnose switch network-monitor dump-l2-db
diagnose switch network-monitor dump-l3-db
diagnose switch network-monitor dump-monitors
diagnose switch network-monitor parser-stats
```

Variable	Description
cfg-stats	Display network-monitoring configuration statistics.
clear-db	Delete all network-monitoring database entries.
dump-l2-db	List all detected devices from the layer-2 database.
dump-l3-db	List all detected devices from the layer-3 database.
dump-monitors	List the monitors used for survey-mode network monitoring.
parser-stats	List the network-monitoring parser statistics.

Example output

```
S524DF4K15000024 # diagnose switch network-monitor cfg-stats
Network Monitor Configuration Statistics:
---------------------------------
Adds         : 1
Deletes      : 0
Free Entries : 19

S524DF4K15000024 # diagnose switch network-monitor dump-monitors
Entry ID       Monitor Type       Monitor MAC      Packet-count
=================================================================
1               directed-mode   00:25:00:61:64:6d       0
2               survey-mode     08:5b:0e:f1:95:e5       0
3               survey-mode     08:5b:0e:f1:95:e5       0
4               survey-mode     08:5b:0e:f1:95:e5       0
5               survey-mode     00:00:5e:00:01:05       0
6               survey-mode     08:5b:0e:f1:95:e5       0
7               survey-mode     00:21:cc:d2:76:72       0
```

```
S524DF4K15000024 # diagnose switch network-monitor parser-stats
Network Monitor Parser Statistics:
---------------------------------
Arp         : 0
Ip          : 0
Udp         : 0
Tcp         : 0
Dhcp        : 0
Eapol       : 0
Unsupported : 0
```

diagnose switch pdu-counters

Use these commands to manage information from switch packet PDU counters:

```
diagnose switch pdu-counters clear
diagnose switch pdu-counters list
```

Variable	Description
clear	Clear switch packet PDU counters.
list	List nonzero switch packet PDU counters.

Example output

```
S524DF4K15000024 # diagnose switch pdu-counters list

primary CPU counters:
packet receive error :        0
Non-zero port counters:
```

diagnose switch physical-ports

Use these commands to display information about physical ports:

```
diagnose switch physical-ports cable-diag <port_name>
diagnose switch physical-ports datarate [<port_list>]
diagnose switch physical-ports io-stats clear-local <port_list>
diagnose switch physical-ports io-stats cumulative
diagnose switch physical-ports io-stats list [<port_list>]
diagnose switch physical-ports linerate [<port_list>]
diagnose switch physical-ports list [<port_name>]
diagnose switch physical-ports mapping
diagnose switch physical-ports mdix-status <port_name>
diagnose switch physical-ports port-stats [<port_list>]
diagnose switch physical-ports qos-stats clear <port_list>
diagnose switch physical-ports qos-stats list [<port_list>]
diagnose switch physical-ports split-status
diagnose switch physical-ports stats clear-local <port_list>
diagnose switch physical-ports stats list [<port_list>]
```

```
diagnose switch physical-ports summary [<port_name>]
diagnose switch physical-ports virtual-wire list
```

Variable	Description
cable-diag <port_name>	Display the results of a time-domain reflectometer (TDR) diagnostic test on the specified port.
datarate [<port_list>]	Display the number of packets received and transmitted on the specified ports as well as the data rate. Use commas to separate ports. If the ports are not specified, the statistics for all ports are displayed.
io-stats clear-local <port_list>	Delete the statistics for input and output packets for the specified ports. Use commas to separate ports. For example: 1,3,4-6
io-stats cumulative	Display the cumulative statistics for input and output packets for all ports.
io-stats list [<port_list>]	List the statistics for input and output packets for the specified ports. If the ports are not specified, the statistics for all ports are displayed.
linerate [<port_list>]	Display the number of packets received and transmitted on the specified ports as well as the line rate. Use commas to separate ports. If the ports are not specified, the statistics for all ports are displayed.
list [<port_name>]	Display the details for the specified port. If the port is not specified, the details for all ports are displayed.
mapping	Display which drivers are associated with which ports.
mdix-status <port_name>	Display whether a specified port is a medium-dependent interface crossover (MDIX) port.
port-stats [<port_list>]	Display statistics for the specified ports. Use commas to separate ports. If the ports are not specified, the statistics for all ports are displayed.
qos-stats list [<port_list>]	Display the QoS statistics for the specified ports. If the ports are not specified, the statistics for all ports are displayed.
split-status	Display information about split ports.
stats clear-local <port_list>	Delete the statistics for received and transmitted packets for the specified ports for only the local session. Use commas to separate ports. For example: 1,3,4-6
stats list [<port_list>]	List the statistics for received and transmitted packets for the specified ports. Use commas to separate ports. If the ports are not specified, the statistics for all ports are displayed.

Variable	Description
summary [<port_name>]	Display a summary about the specified physcial port. If the port is not specified, summaries for all ports are displayed.
virtual-wire list	List all virtual wires.

Example output

```
S524DF4K15000024 # diagnose switch physical-ports cable-diag port1
port1:  cable (4 pairs, length +/- 10 meters)
       pair A Open, length 0 meters
       pair B Open, length 0 meters
       pair C Open, length 0 meters
       pair D Open, length 0 meters

S524DF4K15000024 # diagnose switch physical-ports datarate 1,3,4-6
Rate Display Mode: DATA_RATE
Port       |  TX Packets     |  TX Rate        ||  RX Packets |  RX Rate      |
-------------------------------------------------------------------------------
     port1 |               0 |     0.0000 Mbps ||           0 |   0.0000 Mbps |
     port3 |               0 |     0.0000 Mbps ||           0 |   0.0000 Mbps |
     port4 |               0 |     0.0000 Mbps ||           0 |   0.0000 Mbps |
     port5 |               0 |     0.0000 Mbps ||           0 |   0.0000 Mbps |
     port6 |               0 |     0.0000 Mbps ||           0 |   0.0000 Mbps |
-------------------------------------------------------------------------------
                             |     0.0000 Mbps ||             |   0.0000 Mbps |

ctrl-c to stop

S524DF4K15000024 # diagnose switch physical-ports linerate 1,3,4-6
Rate Display Mode: LINE_RATE
Port      |  TX Packets    |  TX Rate        ||  RX Packets    |  RX Rate        |
-------------------------------------------------------------------------------
    port1 |              0 |     0.0000 Mbps ||              0 |     0.0000 Mbps |
    port3 |              0 |     0.0000 Mbps ||              0 |     0.0000 Mbps |
    port4 |              0 |     0.0000 Mbps ||              0 |     0.0000 Mbps |
    port5 |              0 |     0.0000 Mbps ||              0 |     0.0000 Mbps |
    port6 |              0 |     0.0000 Mbps ||              0 |     0.0000 Mbps |
-------------------------------------------------------------------------------
                           |     0.0000 Mbps ||                |     0.0000 Mbps |

ctrl-c to stop

S524DF4K15000024 # diagnose switch physical-ports list port1
                      diagn
Port(port1) is Admin up, line protocol is down
Interface Type is Serial Gigabit Media Independent Interface(SGMII/SerDes)
Address is 08:5B:0E:F1:95:E6, loopback is not set
MTU 9216 bytes, Encapsulation IEEE 802.3/Ethernet-II
half-duplex, 0 Mb/s, link type is auto
input  : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
```

```
0 unicasts, 0 multicasts, 0 broadcasts, 0 unknowns
output : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
0 unicasts, 0 multicasts, 0 broadcasts
0 fragments, 0 undersizes, 0 collisions, 0 jabbers

S524DF4K15000024 # diagnose switch physical-ports mapping
Unmapped port IDs:
Userspace         |           Driver
Port Name             PortID | Unit   Port   Driver Name
--------------------- ------ | ------ ------ ----------------
port1                      1 |      0      2 ge1
port2                      2 |      0      1 ge0
port3                      3 |      0      3 ge2
port4                      4 |      0      4 ge3
port5                      5 |      0      6 ge5
port6                      6 |      0      5 ge4
port7                      7 |      0      7 ge6
port8                      8 |      0      8 ge7
port9                      9 |      0     10 ge9
port10                    10 |      0      9 ge8
port11                    11 |      0     11 ge10
port12                    12 |      0     12 ge11
port13                    13 |      0     14 ge13
port14                    14 |      0     13 ge12
port15                    15 |      0     15 ge14
port16                    16 |      0     16 ge15
port17                    17 |      0     18 ge17
port18                    18 |      0     17 ge16
port19                    19 |      0     19 ge18
port20                    20 |      0     20 ge19
port21                    21 |      0     22 ge21
port22                    22 |      0     21 ge20
port23                    23 |      0     23 ge22
port24                    24 |      0     24 ge23
port25                    25 |      0     42 xe0
port26                    26 |      0     43 xe1
port27                    27 |      0     44 xe2
port28                    28 |      0     45 xe3
port29                    29 |      0     46 xe4
port30                    30 |      0     50 xe8
internal                  31 |      0      0 cpu0

S524DF4K15000024 # diagnose switch physical-ports mdix-status port1
port1:  MDIX(Crossover)

S524DF4K15000024 # diagnose switch physical-ports port-stats 1

port1 Port Stats:

Rx Bytes:                                          0
Rx Packets:                                        0
Rx Unicasts:                                       0
```

```
Rx NUnicasts:                                0
Rx Multicasts:                               0
Rx Broadcasts:                               0
Rx Discards:                                 0
Rx Errors:                                   0
Rx Oversize:                                 0
Rx Pauses:                                   0
Rx IPMC Dropped:                             0
Rx 64 Octets Packets:                        0
Rx 65-127 Octets Packets:                    0
Rx 128-255 Octets Packets:                   0
Rx 256-511 Octets Packets:                   0
Rx 512-1023 Octets Packets:                  0
Rx 1024-1518 OctetsPackets:                  0
Rx 1519-2047 Octets Packets:                 0
Rx 2048-4095 Octets Packets:                 0
Rx 4096-9216 Octets Packets:                 0
Rx 9217-16383 Octets Packets:                0
Rx L3 Packets:                               0

Tx Bytes:                                    0
Tx Packets:                                  0
Tx Unicasts:                                 0
Tx NUnicasts:                                0
Tx Multicasts:                               0
Tx Broadcasts:                               0
Tx Discards:                                 0
Tx Errors:                                   0
Tx Oversize:                                 0
Tx Pauses:                                   0
Tx IPMC Dropped:                             0
Tx 64 Octets Packets:                        0
Tx 65-127 Octets Packets:                    0
Tx 128-255 Octets Packets:                   0
Tx 256-511 Octets Packets:                   0
Tx 512-1023 Octets Packets:                  0
Tx 1024-1518 Octets Packets:                 0
Tx 1519-2047 Octets Packets:                 0
Tx 2048-4095 Octets Packets:                 0
Tx 4096-9216 Octets Packets:                 0
Tx 9217-16383 Octets Packets:                0

Fragments:                                   0
Undersize:                                   0
Jabbers:                                     0
Collisions:                                  0
CRC Alignment Errors:                        0
IPMC Bridged:                                0
IPMC Routed:                                 0

--------------------------------------------------------------------------------
```

```
S524DF4K15000024 # diagnose switch physical-ports qos-stats list 1

port1 QoS Stats:

queue |     unicast pkts |    unicast bytes |   multicast pkts |  multicast bytes
-------------------------------------------------------------------------------
    0 |                 0 |                0 |                0 |                 0
    1 |                 0 |                0 |                0 |                 0
    2 |                 0 |                0 |                0 |                 0
    3 |                 0 |                0 |                0 |                 0
    4 |                 0 |                0 |                0 |                 0
    5 |                 0 |                0 |                0 |                 0
    6 |                 0 |                0 |                0 |                 0
    7 |                 0 |                0 |                0 |                 0

queue |  ucast drop pkts | ucast drop bytes |  mcast drop pkts | mcast drop bytes
-------------------------------------------------------------------------------
    0 |                 0 |                0 |                0 |                 0
    1 |                 0 |                0 |                0 |                 0
    2 |                 0 |                0 |                0 |                 0
    3 |                 0 |                0 |                0 |                 0
    4 |                 0 |                0 |                0 |                 0
    5 |                 0 |                0 |                0 |                 0
    6 |                 0 |                0 |                0 |                 0
    7 |                 0 |                0 |                0 |                 0
-------------------------------------------------------------------------------

S524DF4K15000024 # diagnose switch physical-ports stats list
Port     | TX Packets |  TX bytes   || RX Packets |  RX Bytes  | RX L3 Packets |
-------------------------------------------------------------------------------
   port1 |          0 |          0 ||           0 |          0 |             0 |
   port2 |          0 |          0 ||           0 |          0 |             0 |
   port3 |          0 |          0 ||           0 |          0 |             0 |
   port4 |          0 |          0 ||           0 |          0 |             0 |
   port5 |          0 |          0 ||           0 |          0 |             0 |
   port6 |          0 |          0 ||           0 |          0 |             0 |
   port7 |          0 |          0 ||           0 |          0 |             0 |
   port8 |          0 |          0 ||           0 |          0 |             0 |
   port9 |          0 |          0 ||           0 |          0 |             0 |
  port10 |          0 |          0 ||           0 |          0 |             0 |
  port11 |          0 |          0 ||           0 |          0 |             0 |
  port12 |          0 |          0 ||           0 |          0 |             0 |
  port13 |          0 |          0 ||           0 |          0 |             0 |
  port14 |          0 |          0 ||           0 |          0 |             0 |
  port15 |          0 |          0 ||           0 |          0 |             0 |
  port16 |          0 |          0 ||           0 |          0 |             0 |
  port17 |          0 |          0 ||           0 |          0 |             0 |
  port18 |          0 |          0 ||           0 |          0 |             0 |
  port19 |          0 |          0 ||           0 |          0 |             0 |
  port20 |          0 |          0 ||           0 |          0 |             0 |
  port21 |          0 |          0 ||           0 |          0 |             0 |
  port22 |          0 |          0 ||           0 |          0 |             0 |
```

```
  port23 |          0 |          0 ||          0 |          0 |          0 |
  port24 |          0 |          0 ||          0 |          0 |          0 |
  port25 |          0 |          0 ||          0 |          0 |          0 |
  port26 |          0 |          0 ||          0 |          0 |          0 |
  port27 |          0 |          0 ||          0 |          0 |          0 |
  port28 |          0 |          0 ||          0 |          0 |          0 |
  port29 |          0 |          0 ||          0 |          0 |          0 |
  port30 |          0 |          0 ||          0 |          0 |          0 |
internal |        393 |    9343000 ||          0 |          0 |          0 |

S524DF4K15000024 # diagnose switch physical-ports summary port1

Portname    Status  Tpid  Vlan  Duplex  Speed  Flags       Discard
__________  ______  ____  ____  ______  _____  __________  _________

port1       down    8100  1     half    -        ,  ,      none

Flags: QS(802.1Q) QE(802.1Q-in-Q,external) QI(802.1Q-in-Q,internal)
TS(static trunk) TF(forti trunk) TL(lacp trunk); MD(mirror dst)
MI(mirror ingress) ME(mirror egress) MB(mirror ingress and egress) CF (Combo
Fiber), CC (Combo Copper)

S524DF4K15000024 # diagnose switch physical-ports virtual-wire list
port7(7) to port8(8) TPID: 0xdee5 VLAN: 70
```

diagnose switch poe status

Use this command to display power over Ethernet (PoE) information for a specific port:

```
diagnose switch poe status <physicial_port_name>
```

Variable	Description
<physicial_port_name>	Enter the port name.

Example output

```
S524DF4K15000024 # diagnose switch poe status port1

Port(1) Power:0.00W,    Power-Status: Searching
Power-Up Mode: Normal Mode
Remote Power Device Type: PD None
Power Class: 0
Defined Max Power: 0.00W, Priority: Low.
Voltage: 54.90V
Current: 0mA
```

diagnose switch trunk list

Use this command to display link aggregation information:

```
diagnose switch trunk list [<trunk_name>]
```

Variable	Description
[<trunk_name>]	Display link aggregation information for the specified trunk. If the trunk is not specified, link aggregation information for all trunks is displayed.

Example output

```
S524DF4K15000024 # diagnose switch trunk list trunk1

Switch Trunk Information, primary-Channel

Trunk Name:  trunk1
Mode:  fortinet-trunk
Port Selection Algorithm:  N/A - Trunk Down
Trunk MAC: 08:5B:0E:F1:95:E6

Active Port  Up  Time
___________  ____________________________

Non-Active Port  Status
_______________  ____________________

port1            BLOCK
port2            BLOCK
```

diagnose switch vlan

Use these commands to display information about virtual LANs:

```
diagnose switch vlan assignment capabilities
diagnose switch vlan assignment ether-proto flush
diagnose switch vlan assignment ether-proto list [{sorted-by-protocol | sorted-by-vlan}]
diagnose switch vlan assignment ipv4 flush
diagnose switch vlan assignment ipv4 list [{sorted-by-address | sorted-by-vlan}]
diagnose switch vlan assignment ipv6 flush
diagnose switch vlan assignment ipv6 list [{sorted-by-address | sorted-by-vlan}]
diagnose switch vlan assignment mac flush
diagnose switch vlan assignment mac list [{sorted-by-mac | sorted-by-vlan}]
diagnose switch vlan info dump
diagnose switch vlan list [<VLAN_ID>]
```

Variable	Description
assignment capabilities	Display information about hardware capabilities for VLAN assignments.
assignment ether-proto flush	Delete all VLAN entries assigned by Ethernet frame type and protocol.
assignment ether-proto list [{sorted-by-protocol | sorted-by-vlan}]	Display VLAN assignments by Ethernet frame type and protocol. Use `sorted-by-protocol` to list VLAN entries by protocol. Use `sorted-by-vlan` to list VLAN entries by the VLAN identifier.
assignment ipv4 flush	Delete all VLAN entries assigned by IPv4 address or subnet.
assignment ipv4 list [{sorted-by-address | sorted-by-vlan}]	Display VLAN assignments by IPv4 address or subnet. Use `sorted-by-address` to list VLAN entries by the mask length and IP address. Use `sorted-by-vlan` to list VLAN entries by the VLAN identifier.
assignment ipv6 flush	Delete all VLAN entries assigned by IPv6 address or subnet.
assignment ipv6 list [{sorted-by-address | sorted-by-vlan}]	Display VLAN assignments by IPv6 address or subnet. Use `sorted-by-address` to list VLAN entries by the mask length and IP address. Use `sorted-by-vlan` to list VLAN entries by the VLAN identifier.
assignment mac flush	Delete all VLAN entries assigned by MAC address.
assignment mac list [{sorted-by-mac | sorted-by-vlan}]	Display VLAN assignments by MAC address. Use `sorted-by-mac` to list VLAN entries by the MAC address. Use `sorted-by-vlan` to list VLAN entries by the VLAN identifier.
info dump	Display VLAN-related information.
list [<VLAN_ID>]	Display which ports are assigned to the specified VLAN identifier. If the VLAN identifier is not specified, the information for all VLAN identifiers is displayed.

Example output

```
S524DF4K15000024 # diagnose switch vlan assignment capabilities
Assignment modes supported:
Port based assignment
IPv4 address/subnet based assignment
IPv6 address/subnet based assignment
MAC address based assignment
Ethernet Protocol based assignment

S524DF4K15000024 # diagnose switch vlan info dump
Ports:
[   port1] Force[disabled]
[   port2] Force[disabled]
[   port3] Force[disabled]
[   port4] Force[disabled]
[   port5] Force[disabled]
```

```
[   port6] Force[disabled]
[   port7] Force[disabled]
[   port8] Force[disabled]
[   port9] Force[disabled]
[  port10] Force[disabled]
[  port11] Force[disabled]
[  port12] Force[disabled]
[  port13] Force[disabled]
[  port14] Force[disabled]
[  port15] Force[disabled]
[  port16] Force[disabled]
[  port17] Force[disabled]
[  port18] Force[disabled]
[  port19] Force[disabled]
[  port20] Force[disabled]
[  port21] Force[disabled]
[  port22] Force[disabled]
[  port23] Force[disabled]
[  port24] Force[disabled]
[  port25] Force[disabled]
[  port26] Force[disabled]
[  port27] Force[disabled]
[  port28] Force[disabled]
[  port29] Force[disabled]
[  port30] Force[disabled]
[internal] Force[disabled]

Private-VLANs:

S524DF4K15000024 # diagnose switch vlan list
VlanId  Ports
______  ________________________________________________
1       port1 port2 port3 port4 port5 port6 port7 port8 port9
              port10 port11 port12 port13 port14 port15 port16 port17
              port18 port19 port20 port21 port22 port23 port24 port25
              port26 port27 port28 port29 port30
4094    internal
```

diagnose sys checkused

Use the following commands to check which tables are using the entry:

```
diagnose sys checkused <path.object.mkey>
```

Variable	Description
<path.object.mkey>	Display which tables use this entry.

Example output

```
S524DF4K15000024 # diagnose sys checkused switch.physical-port.name

may be used by table switch.trunk.members.member-name
may be used by table switch.mirror.dst
may be used by table switch.mirror.src-ingress.name
may be used by table switch.mirror.src-egress.name
may be used by table switch.acl.policy.ingress-interface.member-name
may be used by table switch.acl.policy.action.mirror
may be used by table switch.acl.policy.action.redirect
may be used by table switch.acl.policy.action.redirect-physical-port.member-name
may be used by table switch.acl.policy.action.egress-mask.member-name
may be used by table switch.virtual-wire.first-member
may be used by table switch.virtual-wire.second-member
may be used by table switch.auto-isl-port-group.members.member-name
may be used by table system.admin.dashboard.interface
```

diagnose sys cpuset

Use this command to display information about which CPU set uses a specific process:

```
diagnose sys cpuset <process_ID> <CPU_set_mask>
```

Variable	Description
<process_ID> <CPU_set_mask>	Specify the process identifier and CPU set mask to find out which CPU set uses the process.

diagnose sys csum

Use this command to display the checksum for the specified file:

```
diagnose sys csum <file_name>
```

Variable	Description
<file_name>	Specify the file that you want the checksum for.

diagnose sys dashboard

Use these commands to display SNMP information:

```
diagnose sys dashboard reset
diagnose sys dashboard stats app-usage {clear <user_name> | show <user_name> <application_
    ID> <optional_VDOM>}
diagnose sys dashboard stats content-summary {clear <user_name> | show <user_name> | show-
    details <user_name> <log_type>}
```

```
diagnose sys dashboard stats detection-summary {clear <user_name> | show <user_name> |
    show-details <user_name> <log_type>}
diagnose sys dashboard stats dlp-archive {clear <user_name> | show <user_name>}
diagnose sys dashboard stats log
diagnose sys dashboard stats log-clear
diagnose sys dashboard stats pol-usage {clear <arguments> | show <user_name>]
diagnose sys dashboard stats pol6-usage clear <arguments>
diagnose sys dashboard stats session-top <user_name>
diagnose sys dashboard stats traffic-history <interface_name>
```

Variable	Description
reset	Reset the dashboard configuration to the default setting.
stats app-usage {clear <user_name> | show <user_name> <application_ID> <optional_VDOM>}	Manage statistics about the top application use: • `clear <user_name>` — Delete statistics for the specified user. • `show <user_name> <application_ID> <optional_VDOM>` — Display statistics for the specified user and application. Optionally, you can specify the virtual domain.
stats content-summary {clear <user_name> | show <user_name> | show-details <user_name> <log_type>}	Manage content-summary statistics: • `clear <user_name>` — Delete statistics for the specified user. • `show <user_name>` — Display statistics for the specified user. • `show-details <user_name> <log_type>` — Delete statistics in the specified log for the specified user.
stats detection-summary {clear <user_name> | show <user_name> | show-details <user_name> <log_type>}	Manage detection-summary statistics: • `clear <user_name>` — Delete statistics for the specified user. • `show <user_name>` — Display statistics for the specified user. • `show-details <user_name> <log_type>` — Delete statistics in the specified log for the specified user.
stats dlp-archive {clear <user_name> | show <user_name>}	Manage statistics about the top data loss prevention (DLP) archive use: • `clear <user_name>` — Delete statistics for the specified user. • `show <user_name>` — Display statistics for the specified user.
stats log	Display log statistics.
stats log-clear	Delete log statistics.

Variable	Description
pol-usage {clear <arguments> | show <user_name>]	Manage statistics about the top policy use: • `clear <arguments>` — Delete the specified statistics. • `show <user_name>` — Display statistics for the specified user.
stats pol6-usage clear <arguments>	Delete statistics about the top policy6 use.
stats session-top <user_name>	Display statistics about the top sessions.
stats traffic-history <interface_ name>	Display statistics about the traffic history on the specified interface.

Example output

```
S524DF4K15000024 # diagnose sys dashboard stats content-summary show admin
0 0 0 0
0 0 0
0 0 0 0 0 0
0
50

S524DF4K15000024 # diagnose sys dashboard stats content-summary show-details admin
memory
0

S524DF4K15000024 # diagnose sys dashboard stats detection-summary show admin
0 0 0 0 0 0 0 0 70 9078
50

S524DF4K15000024 # diagnose sys dashboard stats detection-summary show-details
admin memory
0

S524DF4K15000024 # diagnose sys dashboard stats log
Log statistics - per vdom
Sunday     Monday     Tuesday    Wednesday  Thursday   Friday     Saturday
========== ========== ========== ========== ========== ========== ==========
Vdom root
event log:
       0          0          0         45          0          2         29

Log statistics - summary
event log:
       0          0          0         45          0          2         29
```

diagnose sys dayst-info

Use this command to display information about daylight saving time:

```
diagnose sys dayst-info
```

Example output

```
S524DF4K15000024 # diagnose sys dayst-info
The current timezone '(GMT-8:00)Pacific Time(US&Canada).' daylight saving time
starts at Sun Mar  8 02:00:00 1970, ends at Sun Nov  1 01:00:00 1970
```

diagnose sys fan status

Use this command to display fan information:

```
diagnose sys fan status
```

Example output

```
S524DF4K15000024 # diagnose sys fan status

Module    Status

___________________________________
Fan       OK
Fan speed is set to 50.0%.
```

diagnose sys flash

Use these commands to manage flash memory:

```
diagnose sys flash format
diagnose sys flash list [<file>]
```

Variable	Description
format	Format the shared data partition (flash partition 2).
list [<file>]	Display statistics for a file or directory in flash memory. If no file or directory is specified, statistics for all flash memory are returned.

Example output

```
S524DF4K15000024 # diagnose sys flash list
Partition  Image                                TotalSize(KB)  Used(KB)  Use%  Active
(*) 1      S524DF-3.6.3-FW-build0390-171020          53248     22922   43%  Yes
                                                      4096       448   11%  Yes
2                                                     53248         0    0%  No

Flag * : next-boot partition
Image build at Oct 20 2017 17:10:54 for b0390
```

diagnose sys fsw-cloud-mgr

Use these commands to manage the SSL tunnel for FortiSwitch cloud management:.

```
diagnose sys fsw-cloud-mgr close-access-socket
diagnose sys fsw-cloud-mgr shutdown-ssl
```

Variable	Description
close-access-socket	Restart the SSL tunnel between a FortiSwitch and FortiSwitch cloud management by closing the socket.
shutdown-ssl	Restart the SSL tunnel between a FortiSwitch and FortiSwitch cloud management by sending a SSL_SHUTDOWN request.

diagnose sys kill

Use this command to end a specified process:

```
diagnose sys kill <signal_number> <process_ID>
```

Variable	Description
<signal_number> <process_ID>	End the process with the specified signal.

To find out which processes are currently running, see diagnose sys vlan list on page 197.

diagnose sys link-monitor

Use these commands to manage the link monitor:

```
diagnose sys link-monitor interface <entry>
diagnose sys link-monitor launch <entry>
diagnose sys link-monitor status {entry | all}
```

To configure the link health monitor, see config system link-monitor on page 108.

Variable	Description
interface <entry>	Display information about the specified link-monitor entry.
launch <entry>	Manually launch the specified link-monitor entry.
status {entry | all}	Display information about a specified link-monitor entry or all link-monitor entries.

diagnose sys mpstat

Use this command to display information about CPU use:

```
diagnose sys mpstat <delay> <loops>
```

Variable	Description
<delay> <loops>	Display information about the CPU use after the specified number of seconds (default is 5) and for the specified number of loops (default is 1,000,000). If the values for <delay> <loops> are not specified, there is no delay, and the output continues until a key is pressed.

Example output

```
S524DF4K15000024 # diagnose sys mpstat

Gathering data, wait 5 sec, press any key to quit.
..0..1..2..3..4
TIME          CPU    %usr   %nice    %sys  %idle
04:02:59 PM   all    0.00    0.00    5.73   94.27
                0    0.00    0.00   10.87   89.13
                1    0.00    0.00    0.59   99.41
04:02:59 PM          0.00    0.00    0.00    0.00

TIME          CPU    %usr   %nice    %sys  %idle
04:03:04 PM   all    0.00    0.00    6.87   93.13
                0    0.00    0.00   12.75   87.25
                1    0.00    0.00    1.00   99.00
04:03:04 PM          0.00    0.00    0.00    0.00
```

diagnose sys ntp status

Use this command to display the configuration of the Network Time Protocol (NTP) servers:

```
diagnose sys ntp status
```

To configure the NTP servers, see config system ntp on page 109.

diagnose sys pcb temp

Use this command to display the printed circuit board (PCB) temperature:

```
diagnose sys pcb temp
```

Example output

```
S524DF4K15000024 # diagnose sys pcb temp

Module    Status

_____________________________________
Sensor1   42.0 C
```

diagnose sys process

Use this command to display information about a specific process:

```
diagnose sys process <process_ID>
```

Variable	Description
<process_ID>	Display information about the specified process identifier.

To find out which processes are currently running, see diagnose sys vlan list on page 197.

diagnose sys psu status

Use this command to display information about the power supply unit (PSU):

```
diagnose sys psu status
```

Example output

```
S524DF4K15000024 # diagnose sys psu status

PSU1 is OK.
PSU2 is not present.
```

diagnose sys top

Use this command to list the processes currently running on your FortiSwitch:

```
diagnose sys top <delay> <lines>
```

Variable	Description
<delay> <lines>	Enter the number of seconds to delay (the default is 5) and the maximum lines of output (the default is 20).

In the output, the codes displayed on the second output line mean the following:

- U is % of user space applications using CPU. In the example, 0U means 0% of the user space applications are using CPU.
- S is % of system processes (or kernel processes) using CPU. In the example, 0S means 0% of the system processes are using the CPU.
- I is % of idle CPU. In the example, 98I means the CPU is 98% idle.
- T is the total FortiOS system memory in Mb. In the example, 123T means there are 123 Mb of system memory.
- F is free memory in Mb. In the example, 25F means there is 25 Mb of free memory.

Each additional line of the command output displays the following information for each of the processes running on the FortiSwitch (from left to right):

- Process name
- Process identifier
- State that the process is running in. The process state can be:
  - R for running
  - S for sleep
  - Z for zombie
  - D for disk sleep
- Amount of CPU that the process is using. CPU usage can range from 0.0 for a process that is sleeping to higher values for a process that is taking a lot of CPU time.
- Amount of memory that the process is using. Memory usage can range from 0.1 to 5.5 and higher.

Example output

```
S524DF4K15000024 # diagnose sys top 5 5

Run Time:  3 days, 0 hours and 40 minutes
0U, 6S, 94I; 1978T, 1744F
pyfcgid      695      S       0.0     0.7
pyfcgid      791      S       0.0     0.7
pyfcgid      792      S       0.0     0.7
httpsd       696      S       0.0     0.6
cmdbsvr      611      S       0.0     0.6
```

diagnose sys vlan list

Use these commands to display information about configured VLANs:

```
diagnose syst vlan list
```

To configure a VLAN, see config switch vlan on page 81.

diagnose test application

Use these commands to test specific daemons:

```
diagnose test application dnsproxy <test_level>
diagnose test application fpmd <test_level>
diagnose test application radiusd <test_level>
```

```
diagnose test application sflowd <test_level>
diagnose test application snmpd <test_level>
```

Variable	Description
dnsproxy <test_level>	Specify the test level for the DNS proxy daemon: 1. Clear DNS cache 2. Show statistics 3. Dump DNS setting 4. Reload the fully qualified domain name (FQDN) 5. Requery the FQDN 6. Dump the FQDN
fpmd <test_level>	Specify the test level for the hardware offload daemon.
radiusd <test_level>	Specify the test level for the RADIUS daemon: • 2: Clear the RADIUS server database • 3: Show the RADIUS server database • 33: Show the RADIUS server database (with start time) • 4: Show the RADIUS server database information • 9: Check the high availability (HA) context table checksums • 11: Show the HA synchronization connection status • 20: Show the RADIUS server configuration cache • 21: Show the RADIUS server interface configuration cache • 99: Restart
sflowd <test_level>	Specify the test level for the sFlow daemon: • 1: Show collector setting • 2: Show state
snmpd <test_level>	Specify the test level for the SNMP daemon: • 1: Display daemon process identifier • 2: Display SNMP statistics • 3: Clear SNMP statistics • 4: Generate test trap • 99: Restart daemon

Example output

```
S524DF4K15000024 # diagnose test application dnsproxy 2
config: alloc=1
DNS_CACHE: alloc=0
DNS UDP: req=6680, res=0, fwd=26720, hits=0, alloc=0
cur=90 v6_cur=0
DNS TCP: req=0, alloc=0

S524DF4K15000024 # diagnose test application fpmd 2
```

```
L3 egr obj Num: 0 Max: 8192 LastFoundEgrId: 0
Valid: 0 Gw: 0.0.0.0 IfIndex: 0 RefCount: 0 EgrObj: 0 Status: 0
```

diagnose test authserver

Use these commands to test the authentication server:

```
diagnose test authserver cert <arguments>
diagnose test authserver ldap <server_name> <user_name> <password>
diagnose test authserver ldap-digest <arguments>
diagnose test authserver ldap-direct <arguments>
diagnose test authserver ldap-search <arguments>
diagnose test authserver local <arguments>
diagnose test authserver radius <server_name> <chap | pap | mschap | mschap2> <user_name>
    <password>
diagnose test authserver radius-direct <server_name _or_IP_address> <port_number> <secret>
diagnose test authserver tacacs+ <server_name> <user_name> <password>
diagnose test authserver tacacs+-direct <arguments>
```

Variable	Description
cert <arguments>	Test the certificate authentication.
ldap <server_name> <user_name> <password>	Test the connection to an LDAP server. For the server_name, use the name of the LDAP object, not the LDAP server name. Use credentials that you have used in the LDAP object itself.
ldap-digest <arguments>	Test the LDAP HA1 password query.
ldap-direct <arguments>	Test the connection to an LDAP server.
ldap-search <arguments>	Search for an LDAP server.
local <arguments>	Test the local user.
radius <server_name> <chap | pap | mschap | mschap2> <user_name> <password>	Test the connection to the RADIUS server.
radius-direct <server_name _or_IP_ address> <port_number> <secret>	Test the connection to the RADIUS server. For the port number, enter `-1` to use the default port. Otherwise, enter the port number to check.
tacacs+ <server_name> <user_ name> <password>	Test the connection to the TACACS+ server.
tacacs+-direct <arguments>	Test the connection to the TACACS+ server.

diagnose user radius coa

Use this command to display information about RADIUS authentication and RADIUS accounting:

```
diagnose user radius coa
```

To configure RADIUS authentication and RADIUS accounting, see config user radius on page 122.

execute

Use the `execute` commands perform immediate operations on the FortiSwitch:

execute 802-1x clear interface

Use this command to clear all authorizations on a specified interface:

```
execute 802-1x clear interface {internal | port<integer>}
```

Example

This example shows how to remove all authorizations from port 1:

```
execute 802-1x clear interface port1
```

execute acl clear-counter

Use this command to clear the ACL counters associated with the specified policy:

```
execute acl clear-counter <policy-ID>
```

Use this command to clear all ACL counters:

```
execute acl clear-counter
```

execute backup config

Use the `execute backup config` commands to perform a partial backup of the FortiSwitch configuration to a flash disk, FTP server, or TFTP server.

Syntax

```
execute backup config flash <comment>
execute backup config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config tftp <filename_str> <server_ipv4> [<backup_password_str>]
```

Variable	Description
config flash <comment>	Back up the system configuration to the flash disk. Optionally, include a comment.
config ftp <filename_str> <server_ipv4 [:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to an FTP server. Optionally, you can specify a password to protect the saved data.
config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.

Example

This example shows how to perform a partial backup of the FortiSwitch configuration to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fgt.cfg 192.168.1.23
```

execute backup full-config

Use the `execute backup full-config` commands to back up the full FortiSwitch configuration to a TFTP or FTP server.

Syntax

```
execute backup full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_
    int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]
```

Variable	Description
full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the full system configuration to a file on an FTP server. You can optionally specify a password to protect the saved data.
full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Back up the full system configuration to a file on a TFTP server. You can optionally specify a password to protect the saved data.

Example

This example shows how to back up the full FortiSwitch configuration to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup full-config tftp fgt.cfg 192.168.1.23
```

execute backup memory

Use the `execute backup memory` commands to back up the FortiSwitch logs to a TFTP or FTP server.

Syntax

```
execute backup memory alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute backup memory alllogs tftp <server_ipv4>
execute backup memory log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_
    str> <password_str> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}
execute backup memory log tftp <server_ipv4> {app-ctrl | event | ids | im | spam | virus |
    voip | webfilter}
```

Variable	Description
memory alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]	Back up either all memory or all hard disk log files for to an FTP server. The disk option is available on FortiSwitch models that log to a hard disk.
memory alllogs tftp <server_ipv4>	Back up either all memory or all hard disk log files for this FortiSwitch to a TFTP server. he disk option is available on FortiSwitch models that log to a hard disk.
memory log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_str> <password_str> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiSwitch models that log to a hard disk.

Variable	Description
memory log tftp <server_ipv4> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiSwitch models that log to a hard disk.

Example

This example shows how to back up all FortiSwitch log files to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup memory alllogs tftp fgt.cfg 192.168.1.23
```

execute batch

Use the `execute batch` commands to execute a series of CLI commands.

The `execute batch` commands are controlled by the Maintenance (**mntgrp**) access control group.

Syntax

```
execute batch [<cmd_cue>]
```

The parameter <cmd_cue> includes the following values:

- `end` — exit session and run the batch commands
- `lastlog` — read the result of the last batch commands
- `start` — start batch mode
- `status`— batch mode status reporting if batch mode is running or stopped

Example

To start batch mode:

```
   execute batch start
Enter batch mode...
```

To enter commands to run in batch mode:

```
config system global
set refresh 5
end
```

To execute the batch commands:

```
   execute batch end
Exit and run batch commands...
```

execute bpdu-guard

Use this command to reset a port that goes down after receiving a BPDU:

```
execute bpdu-guard reset {internal | port<number>}
```

Example

This example shows how to reset port 1 after it receives a BPDU and goes down:

```
execute bpdu-guard reset port1
```

execute cfg reload

Use this command to restore the saved configuration when the configuration change mode is `manual` or `revert`. This command has no effect if the mode is `automatic`, the default. The `set cfg-save` command in `system global` sets the configuration change mode.

When you reload the saved system configuration, the your session ends and the FortiSwitch performs a restart.

In the default configuration change mode, `automatic`, CLI commands become part of the saved system configuration when you execute them by entering either next or end.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the system restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. You set the timeout in `system global` using the `set cfg-revert-timeout` command.

Syntax

```
execute cfg reload
```

Example

This is sample output from the command when successful:

```
# execute cfg reload
configs reloaded. system will reboot. This is sample output from the command when not in
    runtime-only configuration mode:
# execute cfg reload
no config to be reloaded.
```

execute cfg save

Use this command to save configuration changes when the configuration change mode is `manual` or `revert`. If the mode is `automatic`, the default, all changes are added to the saved configuration as you make them and

this command has no effect. The `set cfg-save` command in `system global` sets the configuration change mode.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the system restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are reverted automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. To change the timeout from the default of 600 seconds, go to `system global` and use the `set cfg-revert-timeout` command.

Syntax

```
execute cfg save
```

Example

This is sample output from the command:

```
# execute cfg save
config saved.
This is sample output when not in runtime-only configuration mode. It also occurs when in
    runtime-only configuration mode and no changes have been made:
# execute cfg save
no config to be saved.
```

execute clear switch igmp-snoop

Use this command to clear the learned and configured multicast groups from the FortiSwitch.

Syntax

```
execute clear switch igmp-snoop
```

execute clear system arp table

Use this command to cslear all the entries in the ARP table.

Syntax

```
execute clear system arp table
```

execute cli check-template-status

Use this command to report the status of the secure copy protocol (SCP) script template.

Syntax

```
execute cli check-template-status
```

execute cli status-msg-only

Use this command to enable or disable the display of standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session.

Syntax

```
execute cli status-msg-only {enable | disable}
```

Variable	Description	Default
status-msg-only {enable | disable}	Enable or disable standardized CLI error output messages. Entering the command without enable or disable disables displaying standardized output.	enable

execute date

Use this command to display or set the system date.

Syntax

```
execute date [<date_str>]
```

date_str has the form `yyyy-mm-dd`, where:

- **yyyy** is the year. The range is: 2001 to 2037
- **mm** is the month. The range is 01 to 12
- **dd** is the day of the month. The range is 01 to 31

If you do not specify a date, the command returns the current system date. Shortened values, such as “06” instead of “2006” for the year or “1” instead of “01” for month or day, are not valid.

Example

This example sets the date to 17 September 2016:

```
execute date 2016-09-17
```

execute dhcp-snooping

Use this command to remove an IP address from the DHCP-snooping client or server database on a specific VLAN:

```
execute dhcp-snooping expire-client <VLAN-ID> <xx:xx:xx:xx:xx:xx>
```

```
execute dhcp-snooping expire-server <VLAN-ID> <xx:xx:xx:xx:xx:xx>
```

Variable	Description	Default
<VLAN-ID>	Enter the VLAN identifier. The value range is 1-4095.	No default
<xx:xx:xx:xx:xx:xx>	Enter the MAC address for the IP address to remove.	No default

Example

This example shows how to remove the IP address that corresponds to VLAN 100 and to the MAC address 01:23:45:67:89:01 from the DHCP-snooping client database:

```
execute dhcp-snooping expire-client 100 01:23:45:67:89:01
```

execute disconnect-admin-session

Use this command to disconnect an administrator who is logged in.

Syntax

```
execute disconnect-admin-session <index_number>
```

To determine the index of the administrator that you want to disconnect, view the list of logged-in administrators with the following command:

```
execute disconnect-admin-session ?
```

The list of logged-in administrators looks like this:

```
Connected:
INDEX   USERNAME     TYPE      FROM               TIME
    0       admin        WEB       172.20.120.51      Mon Aug 14 12:57:23 2006
    1       admin2       CLI       ssh(172.20.120.54) Mon Aug 14 12:57:23 2006
```

Example

This example shows how to disconnect the logged administrator `admin2`:

```
execute disconnect-admin-session 1
```

execute factoryreset

Use this command to reset the FortiSwitch configuration to factory default settings.

Syntax

```
execute factoryreset
```

This procedure deletes all changes that you have made to the FortiSwitch configuration and reverts the system to its original configuration, including resetting interface addresses.

execute flapguard reset

Use this command to reset the specified port if flap guard was triggered on that port:

```
execute flapguard reset <port>
```

Example

This example shows how to reset port 1 after flap guard was triggered on it:

```
execute flapguard reset port1
```

execute interface dhcpclient-renew

Use this command to renew the DHCP client for the specified DHCP interface and close the CLI session. If there is no DHCP connection on the specified port, there is no output.

Syntax

```
execute interface dhcpclient-renew <interface>
```

Example

This is the output for renewing the DHCP client on port 1 before the session closes:

```
# execute interface dhcpclient-renew port1
renewing dhcp lease on port1
```

execute interface pppoe-reconnect

Use this command to reconnect to the PPPoE service on the specified PPPoE interface and close the CLI session. If there is no PPPoE connection on the specified port, there is no output.

Syntax

```
execute interface pppoe-reconnect <interface>
```

execute license add

Use this command to add a new license.

Syntax

```
execute license add <key>
```

execute license enhanced-debugging

Use this command to get information about the enhanced debugging license or to remove it.

Syntax

```
execute license enhanced-debugging {clear | description | get | status}
```

Variable	Description
clear	Remove the current enhanced debugging license key.
description	Get a general description of the enhanced debugging license key.
get	Retrieve the enhanced debugging license key.
status	Check whether the enhanced debugging license is active.

execute license status

Use this command to display the status of all installed licenses.

Syntax

```
execute license status
```

execute log delete

Use this command to clear all traffic log entries in memory. You will be prompted to confirm the command.

Syntax

```
execute log delete
```

execute log delete-all

Use this command to clear all log entries in memory and current log files on hard disk. If your system has no hard disk, only log entries in system memory are cleared. You will be prompted to confirm the command.

Syntax

```
execute log delete-all
```

execute log display

Use this command to display log messages that you have selected with the `execute log filter` command.

Syntax

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the following commands:

```
execute log filter start-line 1
execute log display
```

You can restore the log filters to their default values using the following command:

```
execute log filter reset
```

execute log filter

Use this command to select log messages for viewing or deletion. You can view one log category on one device at a time. Optionally, you can filter the messages to select only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Commands are cumulative. If you omit a required variable, the command displays the current setting.

Use as many `execute log filter` commands as you need to define the log messages that you want to view.

```
execute log filter category <category_name>
execute log filter device {memory | faz | fds}
execute log filter dump
execute log filter field <name>
execute log filter ha-member <unitsn_str>
execute log filter max-checklines <int>
execute log filter reset
execute log filter start-line <line_number>
execute log filter view-lines <count>
```

Variable	Description	Default
category <category_name>	Enter the type of log you want to select. For SQL logging and memory logging, one of: utm, content, event, or traffic	`event`

Variable	Description	Default
device {memory | faz | fds}	Device where the logs are stored.	memory
dump	Display current filter settings.	No default
field <name>	Press Enter to view the fields that are available for the associated category. Enter the fields you want, using commas to separate multiple fields.	No default
ha-member <unitsn_str>	Select logs from the specified HA cluster member. Enter the serial number of the system.	No default
max-checklines <int>	Set maximum number lines to check. Range 100 to 1,000,000. A value of 0 disables the feature.	No default
reset	Execute this command to reset all filter settings.	No default
start-line <line_number>	Select logs starting at specified line number. The value must be 1 or higher.	1
view-lines <count>	Set lines per view. The value range is 5 to 1000.	10

execute log-report reset

Use this command to delete all logs, archives, and user configured report templates.

Syntax

```
execute log-report reset
```

execute loop-guard reset

Use this command to reset a port that has been put out of service by loop-guard.

```
execute loop-guard reset <interface>
```

Example

This example shows how to reset port 1 after loop guard was triggered on it:

```
execute loop-guard reset port1
```

execute mac clear

Use this command to clear MAC addresses.

Syntax

```
execute mac clear all
execute mac clear by-interface <interface>
execute mac clear by-mac-address <mac_address>
execute mac clear by-vlan <vlan_int>
execute mac clear by-vlan-and-interface <vlan_int> <interface>
execute mac clear by-vlan-and-mac-address <vlan_int> <mac_address>
```

Variable	Description
all	Clear all MAC entries.
by-interface <interface>	Clear all MAC entries on the specified interface.
by-mac-address <mac_address>	Clear all MAC entries for a specified MAC address.
by-vlan <vlan_int>	Clear all MAC entries for a specified VLAN.
by-vlan-and-interface <vlan_int> <interface>	Clear all MAC entries for a specified VLAN on a specified interface.
by-vlan-and-mac-address <vlan_int> <mac_address>	Clear all MAC entries for a specified VLAN that match the specified MAC address.

execute mac-limit-violation reset

Use these commands to reset the learning limit violation log.

To enable or disable the learning limit violation log for a FortiSwitch, see config switch global on page 50.

Syntax

```
execute mac-limit-violation reset all
execute mac-limit-violation reset interface <interface_name>
execute mac-limit-violation reset vlan <VLAN_ID>
```

Variable	Description
all	Clear all learning limit violation logs.
interface <interface_name>	Clear the learning limit violation log for a specific interface.
vlan <VLAN_ID>	Clear the learning limit violation log for a specific VLAN.

Example

This example shows how to clear the learning limit violation log for VLAN 5:

```
execute mac-limit-violation reset vlan 5
```

execute ping

The `execute ping` command sends one or more ICMP echo request (ping) to test the network connection between the FortiSwitch and another network device.

Syntax

```
execute ping <address_ipv4>
```

`<address_ipv4>` is an IP address.

Example

This example shows how to ping a host with the IP address 172.20.120.16.

```
#execute ping 172.20.120.16

PING 172.20.120.16 (172.20.120.16): 56 data bytes
64 bytes from 172.20.120.16: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.20.120.16: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=4 ttl=128 time=0.2 ms

--- 172.20.120.16 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

execute ping-options

Use this command to set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiSwitch and another network device.

Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options interval <seconds>
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
data-size <bytes>	Specify the datagram size in bytes.	56
df-bit {yes | no}	Set `df-bit` to `yes` to prevent the ICMP packet from being fragmented. Set `df-bit` to `no` to allow the ICMP packet to be fragmented.	no
interval <seconds>	Specify the number of seconds between two pings. The value must be greater than 0.	No default
pattern <2-byte_hex>	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the `data_size` parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default
repeat-count <repeats>	Specify how many times to repeat ping.	5
source {auto | <source-intf_ip>}	Specify the FortiSwitch interface from which to send the ping. If you specify `auto`, the system selects the source address and interface based on the route to the `<host-name_str>` or `<host_ip>`. Specifying the IP address of a FortiSwitch interface tests connections to different network segments from the specified interface.	auto
timeout <seconds>	Specify, in seconds, how long to wait until ping times out.	2
tos <service_type>	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted: • lowdelay — minimize delay • throughput — maximize throughput • reliability — maximize reliability • lowcost — minimize cost	0
ttl <hops>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes | no}	Select `yes` to validate reply data.	`no`
view-settings	Display the current ping option settings.	No default

Example

Use the following command to increase the number of pings sent:

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiSwitch interface with IP address 192.168.10.23:

```
execute ping-options source 192.168.10.23
```

execute ping6

The ping6 command sends one or more ICMP echo request (ping) to test the network connection between the FortiSwitch and an IPv6-capable network device.

Syntax

```
execute ping6 {<address_ipv6> | <host-name_str>}
```

Example

This example shows how to ping a host with the IPv6 address `12AB:0:0:CD30:123:4567:89AB:CDEF`.

```
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

execute ping6-options

Use this command to set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiSwitch and an IPv6-capable network device.

Syntax

```
execute ping6-options data-size <bytes>
execute ping6-options interval <seconds>
execute ping6-options pattern <2-byte_hex>
execute ping6-options repeat-count <repeats>
execute ping6-options source {auto | <source-intf_ip>}
execute ping6-options timeout <seconds>
execute ping6-options tos <service_type>
execute ping6-options ttl <hops>
execute ping6-options validate-reply {yes | no}
execute ping6-options view-settings
```

Variable	Description	Default
data-size <bytes>	Specify the datagram size in bytes.	56
df-bit {yes | no}	Set `df-bit` to `yes` to prevent the ICMP packet from being fragmented. Set `df-bit` to `no` to allow the ICMP packet to be fragmented.	no
interval <seconds>	Specify the number of seconds between two pings. The value must be greater than 0.	No default
pattern <2-byte_hex>	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the `data_size` parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default

Variable	Description	Default
repeat-count <repeats>	Specify how many times to repeat ping.	5
source {auto | <source-intf_ip>}	Specify the FortiSwitch interface from which to send the ping. If you specify `auto`, the system selects the source address and interface based on the route to the `<host-name_str>` or `<host_ip>`. Specifying the IP address of a FortiSwitch interface tests connections to different network segments from the specified interface.	auto
timeout <seconds>	Specify, in seconds, how long to wait until ping times out.	2
tos <service_type>	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted: • `lowdelay` — minimize delay • `throughput` — maximize throughput • `reliability` — maximize reliability • `lowcost` — minimize cost	0
ttl <hops>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes | no}	Select `yes` to validate reply data.	`no`
view-settings	Display the current ping option settings.	No default

Example

Use the following command to validate reply data:

```
execute ping6-options validate-reply yes
```

execute poe-reset

This command performs a PoE reset on the specified port.

Syntax

```
execute poe-reset <port_number>
```

Example

Use the following command to reset the PoE power on port 1:

```
execute poe-reset port1
```

execute reboot

Use this command to restart the system.

Abruptly powering off your system may corrupt its configuration. Use the `reboot` or `shutdown` commands to ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute reboot [comment "comment_string">]
```

`[comment <"comment_string">]` enables you to optionally add a message that will appear in the hard disk log indicating the reason for the reboot. If the message is more than one word it must be enclosed in quotation marks.

Example

This example shows the reboot command with a message included:

```
execute reboot comment "December monthly maintenance"
```

execute restore

Use this command to restore a configuration, firmware, or IPS signature file. The following options are available:

- restore the configuration from a file
- change the FortiSwitch firmware
- restore the bios from a file

When virtual domain configuration is enabled, the content of the backup file depends on the administrator account that created it.

A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin account can restore the configuration from this file.

A backup file from a regular administrator account contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute restore bios tftp <filename_str> <server_ipv4[:port_int]>
execute restore config flash <revision>
execute restore config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_
    int]> [<username_str> <password_str>] [<backup_password_str>]
execute restore config tftp <filename_str> <server_ipv4> [<backup_password_str>]
execute restore image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
execute restore secondary-image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn
    [:port_int]> [<username_str> <password_str>]
execute restore secondary-image tftp <filename_str> <server_ipv4>
```

Variable	Description
bios tftp <filename_str> <server_ipv4 [:port_int]>	Restore the bios. Download the restore file from a TFTP server.
config flash <revision>	Restore the specified revision of the system configuration from the flash disk.
config ftp <filename_str> <server_ipv4 [:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>] [<backup_password_str>]	Restore the system configuration from an FTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.
config tftp <filename_str> <server_ipv4> [<backup_password_str>]	Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.
image ftp <filename_str> <server_ipv4 [:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]	Download a firmware image from an FTP server to the FortiSwitch. The FortiSwitch reboots, loading the new firmware. This command is not available in multiple VDOM mode.
image management-station <version_ int>	Download a firmware image from the central management station. This is available if you have configured a FortiManager unit as a central management server. This is also available if your account with FortiGuard Analysis and Management Service allows you to upload firmware images.
image tftp <filename_str> <server_ipv4>	Download a firmware image from a TFTP server to the FortiSwitch. The FortiSwitch reboots, loading the new firmware.
secondary-image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn [:port_int]> [<username_str> <password_ str>]	Download a firmware image from an FTP server to the FortiSwitch. The FortiSwitch saves the new firmware image in the secondary image partition.
secondary-image tftp <filename_str> <server_ipv4>	Download a firmware image from a TFTP server to the FortiSwitch. The FortiSwitch saves the new firmware image in the secondary image partition.

Example

This example shows how to upload a configuration file from a TFTP server to the FortiSwitch and restart the FortiSwitch with this configuration. The name of the configuration file on the TFTP server is `backupconfig`. The IP address of the TFTP server is 192.168.1.23.

```
execute restore config tftp backupconfig 192.168.1.23
```

execute revision

Use this command to manage configuration and firmware image files on the local disk.

Syntax

```
execute revision delete config <revision>
execute revision list config
execute revision show config
```

Variable	Description
delete config <revision>	Delete the specified configuration revision on the local disk.
list config	List the configuration revisions on the local disk.
show config	Display the details of the configuration revision on the local disk.

Example

Use the following command to delete revision 1 of the configuration file on the local disk:

```
execute revision delete config 1
```

execute router restart

Use this command to restart the router software:

```
execute router restart
```

execute set-next-reboot

Use this command to start the FortiSwitch with primary or secondary firmware after the next reboot. This command is available on models that can store two firmware images. By default, the FortiSwitch loads the firmware from the primary partition.

Syntax

```
execute set-next-reboot {primary | secondary}
```

Example

Use the following command to start the FortiSwitch with the firmware in the secondary partition:

```
execute set-next-reboot secondary
```

execute shutdown

Use this command to shut down the system immediately. You will be prompted to confirm this command.

Abruptly powering off your system might corrupt its configuration. Using the reboot and shutdown options in the CLI or in the Web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute shutdown [comment <"comment_string">]
```

The comment field is optional. Use it to add a message that will appear in the event log message that records the shutdown. The comment message does not appear on the Alert Message console. If the message is more than one word it must be enclosed in quotation marks.

Example

This example shows the reboot command with a message included.

```
execute shutdown comment "emergency facility shutdown"
```

An event log message similar to the following is recorded:

```
2009-09-08 11:12:31 critical admin 41986 ssh(172.20.120.11) shutdown User admin shutdown
    the device from ssh(172.20.120.11). The reason is 'emergency facility shutdown'
```

execute ssh

Use this command to establish an SSH session with another system.

Syntax

```
execute ssh <destination>
```

`<destination>` is the destination in the form user@ip or user@host.

Example

```
execute ssh admin@172.20.120.122
```

To end an SSH session, type `exit`:

```
FGT-6028030112 # exit
Connection to 172.20.120.122 closed.
FGT-8002805000 #
```

execute stage

Use this command to stage an image from an FTP or TFTP server.

Syntax

```
execute stage image ftp <string> <ftp server>[:ftp port]
execute stage image tftp <string> <ip>
```

`image` is the image file name (including path) on the remote server.

execute sticky-mac

Use this command to manage MAC addresses that were dynamically learned and are persistent when the status of a FortiSwitch port changes (goes down or up).

Syntax

```
execute sticky-mac delete-unsaved {all | interface <interface_name>}
execute sticky-mac save {all | interface <interface_name>}
```

Variable	Description
delete-unsaved {all | interface <interface_name>}	Delete all persistent MAC entries (instead of saving them in the FortiSwitch configuration file) for all interfaces or for the specified interface.
save {all | interface <interface_name>}	Save all persistent MAC entries in the FortiSwitch configuration file for all interfaces or for the specified interface.

execute switch-controller get-conn-status

Use this command to display the status of the FortiLink connection. This command is valid only when the FortiSwitch is managed by a FortiGate.

Syntax

```
execute switch-controller get-conn-status
```

execute system certificate ca

Use this command to import a CA certificate from a TFTP or SCEP server to the FortiSwitch or to export a CA certificate from the FortiSwitch to a TFTP server.

Before using this command, you must obtain a CA certificate issued by a Certificate Authority.

Syntax

```
execute system certificate ca export tftp <name> <file-name> <tftp_ip>
execute system certificate ca import auto <ca_server_url> [ca_identifier_str]
execute system certificate ca import tftp <file-name> <tftp_ip>
```

Variable	Description	Default
import	Import the CA certificate from a TFTP server to the FortiSwitch.	
export	Export or copy the CA certificate from the FortiSwitch to a file on the TFTP server. The available CA certificates are Entrust_802.1x_CA, Entrust_802.1x_G2_CA, Entrust_802.1x_L1K_CA, Fortinet_CA, and Fortinet_CA2.	
<name>	Enter the name of the CA certificate.	
<file-name>	Enter the file name on the TFTP server.	
<tftp_ip>	Enter the TFTP server address.	
auto	Retrieve a CA certificate from a SCEP server.	
tftp	Import the CA certificate to the FortiSwitch from a file on a TFTP server (local administrator PC).	
<ca_server_url>	Enter the URL of the CA certificate server.	
<ca_identifier_str>	CA identifier on CA certificate server (optional).	

execute system certificate crl import auto

Use this command to get a certificate revocation list via LDAP, HTTP, or SCEP protocol, depending on the **autoupdate** configuration.

To use this command, the authentication servers must already be configured.

Syntax

```
execute system certificate crl import auto <crl-name>
```

Variable	Description	Default
import	Import the CRL from the configured LDAP, HTTP, or SCEP authentication server to the FortiSwitch.	

Variable	Description	Default
<crl-name>	Enter the name of the CRL.	
auto	Trigger an auto-update of the CRL from the configured authentication server.	

execute system certificate local export tftp

Use this command to export a local certificate from the FortiSwitch to a TFTP server.

Syntax

```
execute system certificate local export tftp <name> <file-name> <tftp_ip>
```

Variable	Description
export	Export or copy the local certificate from the FortiSwitch to a file on the TFTP server.
<name>	Enter the name of the local certificate. Available local certificates are Entrust_802.1x, Fortinet_Factory, and Fortinet_Firmware.
<file-name>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.

execute system certificate local generate

Use this command to generate a local certificate.

When you generate a certificate request, you create a private and public key pair for the local FortiSwitch. The public key accompanies the certificate request. The private key remains confidential.

When you receive the signed certificate from the CA, use the `system certificate local import` command to install it on the FortiSwitch.

Syntax

```
execute system certificate local generate <name> <key-length> <subject_str> [<optional_
    information>]
```

Variable	Description
<name>	Enter the local certificate name.

Variable	Description
<key-length>	Enter the key size, which can be 1024, 1536, or 2048.
<subject_str>	Enter the subject (host IP address/domain name/e-mail address).
[<optional_information>]	Enter the country name (such as `canada`), country code (such as `ca`), or `null` for none.

execute system certificate local import tftp

Use this command to import a local certificate to the FortiSwitch from a TFTP server.

Syntax

```
execute system certificate local import tftp <file-name> <tftp_ip>
```

Variable	Description	Default
<name>	Enter the name of the local certificate.	
<file-name>	Enter the file name on the TFTP server.	
<tftp_ip>	Enter the TFTP server address.	

execute system certificate remote

Use this command to import a remote certificate from a TFTP server or to export a remote certificate from the FortiSwitch to a TFTP server. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
execute system certificate remote import tftp <file-name> <tftp_ip>
execute system certificate remote export tftp <name> <file-name> <tftp_ip>
```

Variable	Description	Default
import	Import the remote certificate from the TFTP server to the FortiSwitch.	

Variable	Description	Default
export	Export or copy the remote certificate from the FortiSwitch to a file on the TFTP server. To view a list of the certificates, use the following command: `execute system certificate remote export tftp ?`	
<name>	Enter the name of the local certificate.	
<file-name>	Enter the file name on the TFTP server.	
<tftp_ip>	Enter the TFTP server address.	

execute telnet

Use this command to create a Telnet client. You can use this tool to test network connectivity.

Syntax

```
execute telnet <telnet_ipv4>
```

`<telnet_ipv4>` is the address to connect with.

Type `exit` to close the Telnet session.

execute time

Use this command to display or set the system time.

Syntax

```
execute time [<time_str>]
```

time_str has the form **hh:mm:ss,** where:

- **hh** is the hour. The range is 00 to 23.
- **mm** is the minutes. The range is 00 to 59.
- **ss** is the seconds. The range is 00 to 59.

If you do not specify a time, the command returns the current system time.

You are allowed to shorten numbers to only one digit when setting the time. For example both 01:01:01 and 1:1:1 are allowed.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

execute traceroute

Use this command to test the connection between the FortiSwitch and another network device, and display information about the network hops between the FortiSwitch and the device.

Syntax

```
execute traceroute {<ip_address> | <host-name>}
```

Example

This example shows how to test the connection with http://docs.forticare.com. In this example, the traceroute command times out after the first hop indicating a possible problem.

```
#execute traceoute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte packets
1 172.20.120.2 (172.20.120.2) 0.324 ms 0.427 ms 0.360 ms
 2  * * *
```

If your FortiSwitch is not connected to a working DNS server, you will not be able to connect to remote host-named locations with traceroute.

execute tracert6

Use this command to test the connection between the FortiSwitch and another network device using the IPv6 protocol and to display information about the network hops between the FortiSwitch and the device.

Syntax

```
tracert6 [-Fdn] [-f first_ttl] [-i interface] [-m max_ttl]
[-s src_addr] [-q nprobes] [-w waittime] [-z sendwait]
host [paddatalen]
```

Variable	Description
-F	Set the Don't Fragment bit.
-d	Enable debugging.
-n	Do not resolve numeric address to domain name.
-f <first_ttl>	Set the initial time-to-live used in the first outgoing probe packet.
-i <interface>	Select interface to use for tracert.
-m <max_ttl>	Set the max time-to-live (max number of hops) used in outgoing probe packets.

Variable	Description
-s <src_addr>	Set the source IP address to use in outgoing probe packets.
-q <nprobes>	Set the number probes per hop.
-w <waittime>	Set the time in seconds to wait for response to a probe. Default is 5.
-z <sendwait>	Set the time in milliseconds to pause between probes.
host	Enter the IP address or FQDN to probe.
<paddatalen>	Set the packet size to use when probing.

execute upload config

Use this command to upload system configurations to the flash disk from FTP or TFTP sources.

Syntax

```
execute upload config ftp <filename_str> <comment> <server_ipv4[:port_int] | server_fqdn
    [:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]
execute upload config tftp <filename_str> <comment> <server_ipv4>
```

Variable	Description
<comment>	Comment string.
<filename_str>	Filename to upload.
<server_fqdn[:port_int]>	Server fully qualified domain name and optional port.
<server_ipv4[:port_int]>	Server IP address and optional port number.
<username_str>	User name required on server.
<password_str>	Password required on server.
<backup_password_str>	Password for backup file.

execute verify image

Use this command to verify the integrity of the image in the primary or secondary (if applicable) flash partition.

Syntax

```
execute verify image {primary | secondary}
```

Example

```
execute verify image primary

Verifying the image in flash......100%
No issue found!

execute verify image secondary

Verifying the image in flash......100%
Bad/corrupted image found in flash!
Command fail. Return code -1
```

get

The `get` commands provide information about the operation of the FortiSwitch:

- get user ldap on page 279
- get user local on page 280
- get user radius on page 280
- get user setting on page 280
- get user tacacs+ on page 281

get hardware cpu

Use this command to display detailed information about the CPUs installed in your FortiSwitch.

Syntax

```
get hardware cpu
```

Example output

```
S524DF4K15000024 # get hardware cpu

Processor       : ARMv7 Processor rev 0 (v7l)
processor       : 0
BogoMIPS        : 1993.93

processor       : 1
BogoMIPS        : 1993.93

Features        : swp half thumb fastmult edsp tls
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x3
CPU part        : 0xc09
CPU revision    : 0

Hardware        : Broadcom iProc
Revision        : 0000
Serial          : 0000000000000000
```

get hardware memory

Use this command to display information about FortiSwitch memory use. Information includes the total memory, memory in use, and free memory.

Syntax

```
get hardware memory
```

Example output

```
S524DF4K15000024 # get hardware memory
```

```
MemTotal:        2026080 kB
MemFree:         1725840 kB
Buffers:            1336 kB
Cached:            68548 kB
SwapCached:            0 kB
Active:            42724 kB
Inactive:          59596 kB
Active(anon):      32436 kB
Inactive(anon):        0 kB
Active(file):      10288 kB
Inactive(file):    59596 kB
Unevictable:           0 kB
Mlocked:               0 kB
HighTotal:        221184 kB
HighFree:         119468 kB
LowTotal:        1804896 kB
LowFree:         1606372 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:         32436 kB
Mapped:            14680 kB
Shmem:                 0 kB
Slab:              15348 kB
SReclaimable:       3800 kB
SUnreclaim:        11548 kB
KernelStack:         776 kB
PageTables:         3556 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:     1013040 kB
Committed_AS:     594696 kB
VmallocTotal:     245760 kB
VmallocUsed:       66276 kB
VmallocChunk:     163772 kB
```

get hardware status

Report information about the FortiSwitch hardware including ASIC version, CPU type, amount of memory, flash drive size, hard disk size (if present), and USB flash size (if present). Use this information to troubleshoot, to provide to Fortinet Support, or to confirm the features that your FortiSwitch model supports.

Syntax

```
get hardware status
```

Example output

```
S524DF4K15000024 # get hardware status
```

```
Model name: FortiSwitch-524D-FPOE
CPU: ARMv7 Processor rev 0 (v7l)
RAM: 1978 MB
MTD Flash: 52 MB /dev/mtd
Hard disk: not available
Switch CPLD Version: V0.4
Poe Firmware Version:2.6.3
```

get log custom-field

Use this command to get information about custom log fields that have been created. To create custom log fields, see config log custom-field on page 17.

Syntax

```
get log custom-field
```

Example output

```
S524DF4K15000024 # get log custom-field

== [ 1 ]
id: 1
== [ 2 ]
id: 2
```

This output shows that two custom fields have been created.

get log eventfilter

Use this command to find out which logs are enabled:

- Event logs show configuration changes and allow you to monitor the activities administrators perform.
- Router logs allow you to review all router activity. Router logs are available only on supported platforms if you have the advanced features license.
- System logs show system-level activity such as IP conflicts.
- User logs show user activity such as who is logged on and when.

To enable event logging, see config log eventfilter on page 18.

Syntax

```
get log eventfilter
```

Example output

```
S524DF4K15000024 # get log eventfilter

event               : enable
router              : enable
```

```
system                : enable
user                  : enable
```

get log gui

Use this command to find out which device is being used to display logs in the Web-based manager.

Syntax

```
get log gui
```

Example output

```
S524DF4K15000024 # get log gui
log-device            : memory
```

This output shows that logs are being displayed from memory.

get log memory

Use this command to find out the current settings for logging to system memory.

Syntax

```
get log memory filter
get log memory global-setting
get log memory setting
```

Variable	Description
filter	Find out the severity level of log entries made in system memory. The system logs all messages at and above the selected severity level. For example, if the severity is `error`, the system logs `error`, `critical`, `alert`, and `emergency` level messages. • `emergency` — The system is unusable. • `alert` — Immediate action is required. • `critical` — Functionality is affected. • `error` — An erroneous condition exists and functionality is probably affected. • `warning`— Functionality might be affected. • `notification` — Information about normal events. • `information` — General information about system operations. • `debug` — Information used for diagnosing or debugging the system.

Variable	Description
global-setting	Find out the global settings for logging to system memory: • `full-final-warning-threshold` — the number of log entries saved before a final warning is sent. When all memory is filled, the system overwrites the oldest log entries. • `full-first-warning-threshold` — the number of log entries saved before receiving the first warning. • `full-second-warning-threshold` — the number of log entries saved for receiving the second warning. • `hourly-upload` — whether the log is uploaded hourly. • `max-size` — the maximum size of the memory buffer log, in bytes.
setting	Find out the general settings for logging to system memory: • `diskfull` — whether the oldest log entries are overwritten when the system memory is full. • `status` — whether logging to system memory is enabled.

Example output

```
S524DF4K15000024 # get log memory filter
severity            : information

S524DF4K15000024 # get log memory global-setting
full-final-warning-threshold: 95
full-first-warning-threshold: 75
full-second-warning-threshold: 90
hourly-upload       : disable
max-size            : 98304

S524DF4K15000024 # get log memory setting
diskfull            : overwrite
status              : enable
```

get log syslogd

Use this command to get information about your system log 1 settings.

Syntax

```
get log syslogd {filter | setting}
```

Variable	Description
filter	Find out the severity level of system log 1 entries. The system logs all messages at and above the selected severity level. For example, if the severity is `error`, the system logs `error`, `critical`, `alert`, and `emergency` level messages. • `emergency` — The system is unusable. • `alert` — Immediate action is required. • `critical` — Functionality is affected. • `error` — An erroneous condition exists and functionality is probably affected. • `warning`— Functionality might be affected. • `notification` — Information about normal events. • `information` — General information about system operations. • `debug` — Information used for diagnosing or debugging the system.
setting	Find out the general settings for the system log 1: • `diskfull` — whether the oldest log entries are overwritten when the system memory is full. • `status` — whether logging to system memory is enabled.

Example output

```
S524DF4K15000024 # get log syslogd filter
severity            : information

S524DF4K15000024 # get log syslogd setting
status              : disable
```

get log syslogd2

Use this command to get information about your system log 2 settings.

Syntax

```
get log syslogd2 {filter | setting}
```

Variable	Description
filter	Find out the severity level of system log 2 entries. The system logs all messages at and above the selected severity level. For example, if the severity is `error`, the system logs `error`, `critical`, `alert`, and `emergency` level messages. • `emergency` — The system is unusable. • `alert` — Immediate action is required. • `critical` — Functionality is affected. • `error` — An erroneous condition exists and functionality is probably affected. • `warning`— Functionality might be affected. • `notification` — Information about normal events. • `information` — General information about system operations. • `debug` — Information used for diagnosing or debugging the system.
setting	Find out the general settings for the system log 2: • `diskfull` — whether the oldest log entries are overwritten when the system memory is full. • `status` — whether logging to system memory is enabled.

Example output

```
S524DF4K15000024 # get log syslogd2 filter
severity            : information

S524DF4K15000024 # get log syslogd2 setting
status              : disable
```

get log syslogd3

Use this command to get information about your system log 3 settings.

Syntax

```
get log syslogd3 {filter | setting}
```

Variable	Description
filter	Find out the severity level of system log 3 entries. The system logs all messages at and above the selected severity level. For example, if the severity is `error`, the system logs `error`, `critical`, `alert`, and `emergency` level messages. • `emergency` — The system is unusable. • `alert` — Immediate action is required. • `critical` — Functionality is affected. • `error` — An erroneous condition exists and functionality is probably affected. • `warning`— Functionality might be affected. • `notification` — Information about normal events. • `information` — General information about system operations. • `debug` — Information used for diagnosing or debugging the system.
setting	Find out the general settings for the system log 3: • `diskfull` — whether the oldest log entries are overwritten when the system memory is full. • `status` — whether logging to system memory is enabled.

Example output

```
S524DF4K15000024 # get log syslogd3 filter
severity            : information

S524DF4K15000024 # get log syslogd3 setting
status              : disable
```

get router access-list

Use this command to find out if there are any access lists for RIP routing. An access list is a list of IP addresses and the action to take for each one. Access lists provide basic route and network filtering. To create an access list, see config router access-list on page 24.

Syntax

```
get router info access-list
```

Example output

```
S524DF4K15000024 # get router access-list
== [ 1 ]
name: 1
== [ router1 ]
name: router1
== [ mylist ]
name: mylist
```

```
== [ list1 ]
name: list1
```

This output shows that two access lists have beeen created for router1.

get router info bfd neighbor

Use this command to find out where bidirectional forwarding detection (BFD) has been enabled.

Syntax

```
get router info bfd neighbor [detail]
```

Use `detail` to get more detailed output.

Example output

```
S524DF4K15000024 # get router info bfd neighbor

OurAddr          NeighAddr        LD/RD   State    Int
192.168.15.2     192.168.15.1     1/4     UP       vlan2000
192.168.16.2     192.168.16.1     2/2     UP       vlan2001
```

get router info gwdetect

Use this command to get information about the gwdetect status.

Syntax

```
get router info gwdetect
```

get router info kernel

Use this command to get information about the kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

Syntax

```
get router info kernel <routing type>
```

get router info ospf

Use this command to get information about any open shortest path first (OSPF) routing that has been configured. To set up OSPF routing, see config router ospf on page 26.

Syntax

```
get router info ospf {config | database | interface | route | neighbor | border-routers |
    status}
```

Variable	Description
config	Display detailed information about the current OSPF configuration, including interfaces, areas, access lists, and IP addresses.
database	Display information about the OSPF database.
interface	Display information about the OSPF interface.
route	Display the OSPF routing table.
neighbor	Display information about OSPF neighbors.
border-routers	Display information about OSPF border routers.
status	Display the current status of the OSPF routing, including router identifier, flags, timers, and areas.

Example output

```
S524DF4K15000024 # get router info ospf status

OSPF Routing Process, OSPF Router ID: 1.1.1.2
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 5000 millisec(s)
Minimum hold time between consecutive SPFs 10000 millisec(s)
Maximum hold time between consecutive SPFs 10000 millisec(s)
Hold time multiplier is currently 1
SPF algorithm last executed 2d07h22m ago
Last SPF duration 105 usecs
SPF timer is inactive
Refresh timer 10 secs  PacketsSent: 0 PacketsRecv: 0
Number of external LSA 0. Checksum Sum 0x00000000
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 1
Adjacency changes are logged

Area ID: 0.0.0.4 (NSSA)
Shortcutting mode: Default, S-bit consensus: ok
Number of interfaces in this area: Total: 0, Active: 0
It is an NSSA configuration.
Elected NSSA/ABR performs type-7/type-5 LSA translation.
It is not ABR, therefore not Translator.
Number of fully adjacent neighbors in this area: 0
```

```
Area has message digest authentication
Number of full virtual adjacencies going through this area: 0
SPF algorithm executed 1 times
Default-Route Cost: 1
Number of LSA 1
Number of router LSA 1. Checksum Sum 0x0000ebf8
Number of network LSA 0. Checksum Sum 0x00000000
Number of summary LSA 0. Checksum Sum 0x00000000
Number of ASBR summary LSA 0. Checksum Sum 0x00000000
Number of NSSA LSA 0. Checksum Sum 0x00000000
Number of opaque link LSA 0. Checksum Sum 0x00000000
Number of opaque area LSA 0. Checksum Sum 0x00000000
```

get router info rip

Use this command to get information about any Routing Information Protocol (RIP) routing that has been configured. To set up RIP routing, see config router rip on page 34.

Syntax

```
get router info rip {config | database | status}
```

Variable	Description
config	Display detailed information about the current RIP configuration, including keys in the keychain, interfaces, access lists, and IP addresses.
database	Display information about the RIP database.
status	Display the current status of the RIP routing, including filter lists, redistribution, RIP version, and interfaces.

Example output

```
S524DF4K15000024 # get router info rip status

Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 21 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: static
Default version control: send version 2, receive version 2
Interface        Send  Recv   UpdSend Key-chain
vlan35           2     2      9
vlan85           2     2      8
Routing for Networks:
170.38.65.0/24
180.1.1.0/24
```

```
0.0.0.0
Distance: (default is 120)
```

get router info routing-table

Use this command to get information about the routing table.

Syntax

```
get router info routing-table {details <A.B.C.D>| all | rip | ospf | static | connected |
    dump <a.b.c.d>}
```

Variable	Description
details <A.B.C.D>	Display the routing table entries that include the specified IP address or route prefix.
all	Display all routing table entries.
rip	Display the RIP routing table.
ospf	Display the OSPF routing table.
static	Display the routing table entries for static routes.
connected	Display the routing table entries for connected routes.
dump <a.b.c.d>	Display the details of routing table entries that include the specified IP address or route prefix.

Example output

```
S524DF4K15000024 # get router info routing-table details 39.3.2.0
Routing entry for 39.3.2.0/24 using Unicast RIB
Known via "static", distance 10, metric 0, best
* 180.1.1.2, via vlan85

S524DF4K15000024 # get router info routing-table all
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
> - selected route, * - FIB route, ^ - HW install failed

S>*  0.0.0.0/0 [5/0] via 10.105.16.1, mgmt
C>*  10.105.16.0/22 is directly connected, mgmt
S>*  39.3.2.0/24 [10/0] via 180.1.1.2, vlan85
C *  127.0.0.0/8 is directly connected, int1
C>*  127.0.0.0/8 is directly connected, lo
C>*  170.38.65.0/24 is directly connected, vlan35
C>*  180.1.1.0/24 is directly connected, vlan85
C>*  192.168.1.0/24 is directly connected, mgmt
```

```
S524DF4K15000024 # get router info routing-table static
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
> - selected route, * - FIB route, ^ - HW install failed

S>*  0.0.0.0/0 [5/0] via 10.105.16.1, mgmt
S>*  39.3.2.0/24 [10/0] via 180.1.1.2, vlan85

S524DF4K15000024 # get router info routing-table connected
Codes: K - kernel route, C - connected, S - static, R - RIP,
O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel,
> - selected route, * - FIB route, ^ - HW install failed

C>*  10.105.16.0/22 is directly connected, mgmt
C *  127.0.0.0/8 is directly connected, int1
C>*  127.0.0.0/8 is directly connected, lo
C>*  170.38.65.0/24 is directly connected, vlan35
C>*  180.1.1.0/24 is directly connected, vlan85
C>*  192.168.1.0/24 is directly connected, mgmt

S524DF4K15000024 # get router info routing-table dump 10.105.16.0
5:10.105.16.0,6:22,1:unicast,0:connected,7:0,8:0,2:>,3:*,9:direct,11:mgmt
```

get router info vrrp

Use this command to get information about Virtual Router Redundancy Protocol (VRRP) groups.

Syntax

```
get router info vrrp
```

Example output

```
S524DF4K15000024 # get router info vrrp

Interface: vlan-8, primary IP address: 10.10.10.1
UseVMAC: 1
VRID: 5
vrip: 11.1.1.100, priority: 255, state: MASTER
adv_interval: 1, preempt: 1, start_time: 3
vrmac: 00:00:5e:00:01:05
vrdst:
vrgrp: 50
```

get router key-chain

Use this command to get a list of keychains for RIP version 2 routing.

To create a keychain, see config router key-chain on page 25.

Syntax

```
get router key-chain
```

Example output

```
S524DF4K15000024 # get router key-chain
== [ keychain1 ]
name: keychain1
```

get router ospf

Use this command to get information about any open shortest path first (OSPF) routing that has been configured. To set up OSPF routing, see config router ospf on page 26.

Syntax

```
get router ospf
```

Example output

```
S524DF4K15000024 # get router ospf
router-id           : 1.1.1.2
abr-type            : cisco
distance-external   : 0
distance-inter-area : 0
distance-intra-area : 0
default-information-originate: disable
default-information-metric: 10
default-information-metric-type: 2
default-information-route-map: (null)
distance            : 110
rfc1583-compatible  : disable
spf-timers          : 5 10
bfd                 : disable
log-neighbour-changes: enable
area:
== [ 0.0.0.4 ]
id: 0.0.0.4
ospf-interface:
== [ oi1 ]
name: oi1
network:
passive-interface:
distribute-list:
redistribute:
== [ connected ]
name: connected            status: enable            metric: 10
routemap: (null)
== [ static ]
name: static            status: disable            metric: 10           routemap:
(null)
```

```
== [ rip ]
name: rip            status: disable            metric: 10           routemap:
(null)
```

get router prefix-list

Use this command to find out which prefix lists are available for RIP routing. A prefix is an IP address and netmask. A prefix lists specifies the prefixes to allow or deny. To create a prefix list, see config router prefix-list on page 33.

Syntax

```
get router prefix-list
```

Example output

```
S524DF4K15000024 # get router prefix-list
```

```
== [ 2 ]
name: 2
== [ 3 ]
name: 3
```

get router rip

Use this command to get information about any Routing Information Protocol (RIP) routing that has been configured. To set up RIP routing, see config router rip on page 34.

Syntax

```
get router rip
```

Example output

```
S524DF4K15000024 # get router rip
```

```
bfd                  : disable
default-information-originate: disable
default-metric       : 1
distance:
== [ 4 ]
id: 4           prefix: 0.0.0.0 0.0.0.0
distribute-list:
garbage-timer        : 120
interface:
== [ vlan35 ]
name: vlan35             auth-keychain: (null)           auth-mode: text
receive-version: global             send-version: global            split-horizon-
status: enable             split-horizon: regular
neighbor:
== [ 5 ]
```

```
id: 5           ip: 0.0.0.0
network:
== [ 1 ]
id: 1           prefix: 170.38.65.0 255.255.255.0
== [ 2 ]
id: 2           prefix: 180.1.1.0 255.255.255.0
offset-list:
passive-interface:
redistribute:
== [ connected ]
name: connected            status: disable            metric: 0
routemap: (null)
== [ static ]
name: static            status: enable            metric: 0           routemap:
(null)
== [ ospf ]
name: ospf            status: disable            metric: 0           routemap:
(null)
timeout-timer       : 180
update-timer        : 30
version             : 2
```

get router route-map

Use this command to list available route maps for OSPF or RIP routing. To create a route map, see config router route-map on page 39.

Syntax

```
get router route-map
```

Example output

```
S524DF4K15000024 # get router route-map
== [ myroutemap ]
name: myroutemap    protocol: rip
```

get router setting

Use this command to find out which routing protocol is being used by each route map. To assign a route map, see config router setting on page 40.

Syntax

```
get router setting
```

Example output

```
S524DF4K15000024 # get router setting

filter-list:
== [ 1 ]
id: 1           protocol: rip            route-map: myroutemap
== [ 2 ]
id: 2           protocol: ospf            route-map: myroutemap
```

get router static

Use this command to list static routes. To create a static route, see config router static on page 41.

Syntax

```
get router static
```

Example output

```
S524DF4K15000024 # get router static

== [ 1 ]
seq-num: 1
```

get switch acl

Use this command to display the ACL settings.

Syntax

```
get switch acl {counters <policy-id> | policer | policy | service custom | settings |
    usage}
```

Variable	Description
counters <policy-id>	Display information about ACL policies.
policer	List which ACL policers are available for different types of traffic.
policy	Display information about the ACL policy.
service custom	Display a list of preconfigured service entries .
settings	Display the global ACL settings for the FortiSwitch.
usage	Display how much of available resources are used by ACL.

Example output

```
S524DF4K15000024 # get switch acl policer
== [ 1 ]
id: 1   description: policer1

S524DF4K15000024 # get switch acl settings
density-mode        : disable
trunk-load-balance  : enable

S524DF4K15000024 # get switch acl usage

Device    RULES          COUNTERS       POLICERS
               (total/free)   (total/free)  (total/free)
_____________________________________________________________

0         2048  /2034   4096  /8182   4096  /4096
```

get switch dhcp-snooping

Use this command to display more information about the DHCP-snooping database.

Syntax

```
get switch dhcp-snooping {client-db-details | database-summary | limit-db-details |
    server-db-details}
```

Variable	Description
client-db-details	Display details about the DHCP-snooping client database.
database-summary	List the number of VLANs with various features enabled, list trusted and untrusted ports, and report how much of the databases are used.
limit-db-details	Display details about the DHCP-snooping lease-count database.
server-db-details	Display details about the DHCP-snooping server database.

Example output

```
S524DF4K15000024 # get switch dhcp-snooping database-summary

snoop-enabled-vlans             : 10
verifysrcmac-enabled-vlans      : 10
option82-enabled-vlans          : 10
option82-trust-enabled-intfs    :
trusted ports    :
untrusted ports  : port1 port2 port3 port4 port5 port6 port9 port10 port11 port12
               port13 port14 port15 port16 port17 port18 port19 port20 port21 port22
               port23 port24 port25 port26 port27 port28 port29 port30
Client Database          : 0 / 8000
```

```
Server Database           : 0 / 1024
Limit Database            : 0 / 256
```

```
FS1D243Z14000027 # get switch dhcp-snooping client-db-details

       mac        vlan     ip     lease(sec) expiry(sec) interface hostname  domainname     vendor
00:01:00:00:00:01 100 xxx.x.x.xxx   86400       86398      port3
00:03:00:00:00:03 100 xxx.x.x.x     86400       86394      port5
00:03:00:00:00:04 100 xxx.x.x.x     86400       86394      port5   >

FS1D243Z14000027 # get switch dhcp-snooping server-db-details

mac             vlan    ip     interface status first-seen (sec) last-seen (sec) ACK  NAC  OFFER OTHER
00:11:01:00:00:01 30 192.168.5.2  port6  trusted   1503357551         0           12    0      8    0
```

get switch flapguard settings

Use this command to display the flap guard settings.

Syntax

```
get switch flapguard settings
```

Example output

```
S524DF4K15000024 # get switch flapguard settings

flap-duration       : 30
flap-rate           : 5
status              : disable
```

get switch global

Use this command to get information about the global settings of your FortiSwitch.

Syntax

```
get switch global
```

Example output

```
S524DF4K15000024 # get switch global

name                : (null)
mac-aging-interval  : 150
poe-alarm-threshold : 40
poe-power-mode      : first-come-first-served
poe-guard-band      : 10
ip-mac-binding      : enable
dmi-global-all      : enable
poe-pre-standard-detect: enable
poe-power-budget    : 200
```

```
trunk-hash-mode     : enhanced
trunk-hash-unkunicast-src-dst: enable
auto-fortilink-discovery: enable
auto-isl            : enable
mclag-peer-info-timeout: 300
auto-isl-port-group : 0
max-path-in-ecmp-group: 4
virtual-wire-tpid   : 0xdee5
loop-guard-tx-interval: 15
dhcp-snooping-database-export: enable
forti-trunk-dmac    : 02:80:c2:00:00:02
port-security:
link-down-auth      : set-unauth
reauth-period       : 60
max-reauth-attempt  : 2
```

get switch igmp-snooping

Use this command to get the IGMP-snooping settings of your FortiSwitch.

Syntax

```
get switch igmp-snooping {globals | group | interface | static-group}
```

Variable	Description
globals	Display the global IGMP-snooping configuration on the FortiSwitch.
group	Display a list of learned multicast groups.
interface	Display the configured IGMP-snooping interfaces and their current state
static-group	Display the list of configured static groups.

Example output

```
FS1D243Z13000023 # get switch igmp-snooping globals
aging-time : 300
flood-unknown-multicast: disabled

FS1D243Z13000023 # get switch igmp-snooping group
Number of Groups: 7
port of-port VLAN GROUP Age
(__port__9) 1 23 231.8.5.4 16
(__port__9) 1 23 231.8.5.5 16
(__port__9) 1 23 231.8.5.6 16
(__port__9) 1 23 231.8.5.7 16
(__port__9) 1 23 231.8.5.8 16
(__port__9) 1 23 231.8.5.9 16
(__port__9) 1 23 231.8.5.10 16
(__port__43) 3 23 querier 17
```

```
(__port__14) 8 --- flood-reports ---
(__port__10) 2 --- flood-traffic ---

FS1D243Z13000023 # get switch igmp static-group

VLAN ID Group-Name     Multicast-addr  Member-interface
_______ _____________ _______________ ____________________________
11      g239-1        239:1:1:1       port6 trunk-2
11      g239-11       239:2:2:11      port26 port48 trunk-2
40      g239-1        239:1:1:1       port5 port25 trunk-2
40      g239-2        239:2:2:2       port25 port26
```

get switch interface

Use this command to get information about the interfaces, including the class of service (CoS) value, whether sFlow is enabled on the interface, and whether dynamically learned MAC addresses are persistent on the interface.

Syntax

```
get switch interface
```

Example output

```
S524DF4K15000024 # get switch interface

== [ port1 ]
name: port1    sflow-sampler: disabled    port-security:
default-cos: 0   sticky-mac: disable
== [ port2 ]
name: port2    sflow-sampler: disabled    port-security:
default-cos: 0   sticky-mac: disable
== [ port3 ]
name: port3    sflow-sampler: disabled    port-security:
default-cos: 0   sticky-mac: disable
...
```

get switch ip-mac-binding

Use this command to get information about IP MAC binding.

Syntax

```
get switch ip-mac-binding
```

Example output

```
get switch ip-mac-binding

== [ 1 ]
seq-num: 1
```

get switch lldp

Use this command to get information about LLDP.

Syntax

```
get switch lldp {auto-isl-status | neighbors-detail <physical port name>| neighbors-
    summary | profile | settings | stats}
```

Variable	Description
auto-isl-status	Display statistics and staus for the automatic ISL configuration.
neighbors-detail <physical port name>	Display details about a specific LLDP port.
neighbors-summary	Display a summary of LLDP neighbors.
profile	Display the name of available LLDP profiles.
settings	Display whether LLDP is enabled globally, the number of tx-intervals before the local LLDP data expires, the frequency of LLDP PDU transmission, how often the FortiSwitch transmits the first four LLDP packets when a link comes up, and the primary management interface advertised in LLDP and CDP PDUs.
stats	Display the number of packets transmitted, received, and discarded; the number of neighbors added, deleted, and expired; and the number of unknown TLVs.

Example output

```
S524DF4K15000024 # get switch lldp profile
== [ default ]
name: default    802.1-tlvs:    802.3-tlvs:    med-tlvs: inventory-management net-
work-policy
== [ default-auto-isl ]
name: default-auto-isl    802.1-tlvs:    802.3-tlvs:    med-tlvs:
== [ 1 ]
name: 1    802.1-tlvs:    802.3-tlvs:    med-tlvs: inventory-management network-
policy
== [ Forti670i ]
name: Forti670i    802.1-tlvs:    802.3-tlvs:    med-tlvs: inventory-management
network-policy

S524DF4K15000024 # get switch lldp settings
status               : enable
tx-hold              : 8
tx-interval          : 2000
fast-start-interval  : 3
management-interface: internal
```

get switch mac-limit-violations

Use this command to see the first MAC address that exceeded the learning limit for an interface or VLAN.

To enable the learning limit violation log for a FortiSwitch, see config switch global on page 50.

Syntax

```
get switch mac-limit-violations {all | interface <interface_name> | vlan <VLAN_ID>}
```

Variable	Description
all	Display the first MAC address that exceeded the learning limit on any interface or VLAN. An asterisk by the interface name indicates that the interface-based learning limit was exceeded. An asterisk by the VLAN identifier indicates the VLAN-based learning limit was exceeded.
interface <interface_name>	Display the first MAC address that exceeded the learning limit on a specific interface
vlan <VLAN_ID>	Display the first MAC address that exceeded the learning limit on a specific VLAN.

Example output

```
S524DF4K16000028 # get switch mac-limit-violations all
Port            VLAN ID         MAC Address               Timestamp
-------------------------------------------------------------------------------
port3*          5               00:00:01:00:00:01         2017-12-05 15:55:20
port15          9*              0a:c1:08:bf:cc:80         2017-12-05 15:55:44

S524DF4K16000028 # get switch mac-limit-violations interface port3
Port            VLAN ID         MAC Address               Timestamp
-------------------------------------------------------------------------------
port3*          5               00:00:01:00:00:01         2017-12-05 15:55:20

S524DF4K16000028 # get switch mac-limit-violations vlan 9
Port            VLAN ID         MAC Address               Timestamp
-------------------------------------------------------------------------------
port15          9*              0a:c1:08:bf:cc:80         2017-12-05 15:55:44
```

get switch mirror

Use this command to get information about the mirror settings of your FortiSwitch. To configure a port mirror, see config switch mirror on page 62.

Syntax

```
get switch mirror
```

Example output

```
# get switch mirror

dst : (null)
status : inactive
switching-packet : disable
```

get switch modules

Use this command to get information about the modules in your FortiSwitch.

Syntax

```
get switch modules {detail | limits | status | summary} [<port>]
```

Variable	Description
detail [<port>]	Display module details for a specific port or all available ports.
limits [<port>]	Display module limits for a specific port or all available ports.
status [<port>]	Display module status for a specific port or all available ports.
summary [<port>]	Display summary information of all modules for a specific port or all available ports.

Example output

```
FS108D3W14000720 # get switch modules detail port10
_____________________________________________________________
Port(port10)
identifier SFP/SFP+
connector Unk (0x00)
transceiver 1000-Base-T
encoding 8B/10B
Length Decode Common
length_smf_1km N/A
length_cable 100 meter
SFP Specific
length_smf_100m N/A
length_50um_om2 N/A
length_62um_om1 N/A
length_50um_om3 N/A
vendor FINISAR CORP.
vendor_oid 0x009065
vendor_pn FCLF-8521-3
vendor_rev A
vendor_sn PBR1X35
manuf_date 06/20/2007

FS108D3W14000720 # get switch modules status port9
_____________________________________________________________
```

```
Port(port9)
alarm_flags 0x0040
warning_flags 0x0040
temperature 18.792969 C
voltage 3.315100 volts
laser_bias 0.750800 mAmps
tx_power -2.502637 dBm
rx_power -40.000000 dBm
options 0x000F ( TX_DISABLE TX_FAULT RX_LOSS TX_POWER_LEVEL1 )
options_status 0x000C ( RX_LOSS TX_POWER_LEVEL1 )
```

get switch network-monitor

Use this command to get information about network monitoring on the FortiSwitch.

Syntax

```
get switch network-monitor {directed | settings}
```

Variable	Description
directed	List the static entries for network monitoring on the switch.
settings	Display the global settings for network monitoring on the switch.

Example output

```
S524DF4K15000024 # get switch network-monitor directed
== [ 1 ]
id: 1

S524DF4K15000024 # get switch network-monitor settings
db-aging-interval   : 3600
status              : disable
survey-mode         : disable
survey-mode-interval: 120
```

get switch phy-mode

Use this command to find out which split ports have been configured. to configure split ports, see config switch phy-mode on page 64.

Syntax

```
get switch phy-mode
```

Example output

```
S524DF4K15000024 # get switch phy-mode
```

```
port29-phy-mode     : 1x40G
port30-phy-mode     : 1x40G
```

get switch physical-port

Use this command to get information about the physical ports of your FortiSwitch. To configure physical ports, see config switch physical-port on page 66.

Syntax

```
get switch physical-port
```

Example output

```
S524DF4K15000024 # get switch physical-port
== [ port1 ]
name: port1    egress-drop-mode: enabled    link-status: down   status: up
== [ port2 ]
name: port2    egress-drop-mode: enabled    link-status: down   status: up
== [ port3 ]
name: port3    egress-drop-mode: enabled    link-status: down   status: up
...
```

get switch poe inline

Use this command to get information about the system's power over Ethernet (PoE) functions.

Syntax

```
get switch poe inline
```

Example output

```
S524DF4K15000024 # get switch poe inline

Unit Power Budget: 10.00W
Unit Guard Band: 10.00W
Unit Power Consumption: 0.00W
Unit Poe Power Mode : First come first served based.

Interface   Status    State         Max-Power(W)    Power-consumption(W)Class Error
-------------------------------------------------------------------------------
port1       Enabled   Searching         0.00            0.00                  0
port2       Enabled   Searching         0.00            0.00                  0
port3       Enabled   Searching         0.00            0.00                  0
port4       Enabled   Searching         0.00            0.00                  0
port5       Enabled   Searching         0.00            0.00                  0
port6       Enabled   Searching         0.00            0.00                  0
port7       Enabled   Searching         0.00            0.00                  0
port8       Enabled   Searching         0.00            0.00                  0
```

```
port9       Enabled   Searching         0.00            0.00                  0
port10      Enabled   Searching         0.00            0.00                  0
port11      Enabled   Searching         0.00            0.00                  0
port12      Enabled   Searching         0.00            0.00                  0
port13      Enabled   Searching         0.00            0.00                  0
port14      Enabled   Searching         0.00            0.00                  0
port15      Enabled   Searching         0.00            0.00                  0
port16      Enabled   Searching         0.00            0.00                  0
port17      Enabled   Searching         0.00            0.00                  0
port18      Enabled   Searching         0.00            0.00                  0
port19      Enabled   Searching         0.00            0.00                  0
port20      Enabled   Searching         0.00            0.00                  0
port21      Enabled   Searching         0.00            0.00                  0
port22      Enabled   Searching         0.00            0.00                  0
port23      Enabled   Searching         0.00            0.00                  0
port24      Enabled   Searching         0.00            0.00                  0
```

get switch qos

Use this command to get information about the QoS configuration:

Syntax

```
get switch qos (dot1p-map | ip-dscp-map | qos-policy)
```

Variable	Description
dot1p-map	List the available dot1p maps, as well as the CoS values.
ip-dscp-map	List the available DSCP maps.
qos-policy	List the available QoS policies.

Example output

```
S524DF4K15000024 # get switch qos dot1p-map
== [ test1 ]
name: test1    priority-0: queue-2    priority-1: queue-0    priority-2: queue-1
 priority-3: queue-3    priority-4: queue-4    priority-5: queue-5    priority-6:
queue-6    priority-7: queue-7

S524DF4K15000024 # get switch qos ip-dscp-map
== [ m1 ]
name: m1

S524DF4K15000024 # get switch qos qos-policy
== [ default ]
name: default
== [ policy1 ]
name: policy1
```

get switch security-feature

Use this command to display the security-feature settings. To configure security checks for incoming TCP/UDP packets, see config switch security-feature on page 72.

Syntax

```
get switch security-feature
```

Example output

```
S524DF4K15000024 # get switch security-feature

sip-eq-dip           : enable
tcp-flag             : enable
tcp-port-eq          : enable
tcp-flag-FUP         : enable
tcp-flag-SF          : enable
v4-first-frag        : enable
udp-port-eq          : enable
tcp-hdr-partial      : enable
macsa-eq-macda       : enable
allow-mcast-sa       : enable
allow-sa-mac-all-zero: enable
```

get switch static-mac

Use this command to display the static MAC addresses.

Syntax

```
get switch static-mac
```

Example output

```
S524DF4K15000024 # get switch static-mac

== [ 1 ]
seq-num: 1   interface: port5    mac: 00:21:cc:d2:76:72   vlan-id: 35
```

get switch storm-control

Use this command to display storm control settings on your FortiSwitch. To configure storm control, see config switch storm-control on page 74.

Syntax

```
get switch storm-control
```

Example output

```
S524DF4K15000024 # get switch storm-control

broadcast           : enable
rate                : 1000
unknown-multicast   : enable
unknown-unicast     : enable
```

get switch stp instance

Use this command to get information about STP instances on your FortiSwitch. To configure an STP instance, see config switch stp instance on page 75.

Syntax

```
get switch stp instance
```

Example output

```
# get switch stp instance
== [ 0 ]
id: 0
== [ 1 ]
id: 1
```

get switch stp settings

Use this command to get information about STP settings on your FortiSwitch. To configure STP settings, see config switch stp settings on page 76.

Syntax

```
get switch stp settings
```

Example output

```
S524DF4K15000024 # get switch stp settings

forward-time        : 15
hello-time          : 5
max-age             : 20
max-hops            : 20
name                : region1
revision            : 1
status              : enable
```

get switch trunk

Use this command to get information about which trunks on the FortiSwitch have been configured for link aggregation. To configure link aggregation, see config switch trunk on page 77.

Syntax

```
get switch trunk
```

Example output

```
# get switch trunk
== [ 1 ]
name: 1 members:
== [ port3 ]
member-name: port3
== [ port10 ]
member-name: port10
== [ port1 ]
member-name: port1
```

get switch virtual-wire

Virtual wire allows you to forward traffic between two ports with minimal filtering or packet modifications. To configure a virtual wire, see config switch virtual-wire on page 80.

Syntax

```
get switch virtual-wire
```

Example output

```
S524DF4K15000024 # get switch virtual-wire

== [ 1 ]
name: 1
```

get switch vlan

Use this command to get information about VLANs on the FortiSwitch. To configure a VLAN, see config switch vlan on page 81.

Syntax

```
get switch vlan
```

Example output

```
# get switch vlan
== [ 1 ]
```

```
id: 1 private-vlan-type: primary isolated-vlan: 2 community-vlans: 3
== [ 2 ]
id: 2 private-vlan-type: isolated sub-VLAN primary-vlan: 1
== [ 3 ]
id: 3 private-vlan-type: community sub-VLAN primary-vlan: 1
```

get system accprofile

Use this command to view a list of all the system administration access groups. To add an access profile group, see config system accprofile on page 84.

Syntax

```
get system admin accprofile
```

Example output

```
S524DF4K15000024 # get system accprofile

== [ prof_admin ]
name: prof_admin
== [ profile1 ]
name: profile1
```

get system admin list

Use this command to view a list of all the current administration sessions.

Syntax

```
get system admin list
```

Example output

```
# get system admin list

username local  device                   remote               started
admin    sshv2  port1:172.20.120.148:22  172.20.120.16:4167   2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443 172.20.120.161:56365 2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443 172.20.120.16:4214   2006-08-09 12:25:29
```

Variable	Description
username	Name of the admin account for this session
local	The protocol this session used to connect to the system.
device	The interface, IP address, and port used by this session to connect to the system.

Variable	Description
remote	The IP address and port used by the originating computer to connect to the system.
started	The time the current session started.

get system admin status

Use this command to view the status of the currently logged in admin and their session. To configure an administrator account, see config system admin on page 85.

Syntax

```
get system admin status
```

Example Output

```
# get system admin status

username: admin
login local: sshv2
login device: port1:172.20.120.148:22
login remote: 172.20.120.16:4167
login vdom: root
login started: 2006-08-09 12:24:20
current time: 2006-08-09 12:32:12
```

Variable	Description
username	Name of the admin account currently logged in.
login local	The protocol used to start the current session.
login device	The login information from the FortiSwitch including interface, IP address, and port number.
login remote	The computer the user is logging in from including the IP address and port number.
login vdom	The virtual domain the admin is current logged into.
login started	The time the current session started.
current time	The current time of day on the system

get system arp

Use this command to view the ARP table entries on the FortiSwitch. To manually add ARP table entries to the FortiSwitch, see config system arp-table on page 88.

Syntax

```
get system arp
```

Example output

```
S524DF4K15000024 # get system arp

Address           Age(min)    Hardware Addr      Interface
10.105.16.1       0           90:6c:ac:15:2f:94  mgmt
11.1.1.100        -           00:00:5e:00:01:05  vlan-8 (proxy)
```

get system arp-table

Use this command to view the ARP tables on the FortiSwitch.

Syntax

```
get system arp-table
```

Example output

```
# get system arp-table
== [ 1 ]
id: 1 interface: internal ip: 10.10.10.10 mac: 01:02:03:04:05:aa
```

get system auto-update

Use this command to get information about automatic updates.

Syntax

```
get system auto-update {status | versions}
```

Variable	Description
status	Display the status of automatic updates.
versions	Display object versions.

Example output

```
S524DF4K15000024 # get system auto-update status
```

```
FDN availability:  unknown at Wed Dec 31 17:00:00 1969

Push update: disable
Scheduled update: enable
Update daily:   1:00
Server override: disable
Push address override: disable
Web proxy tunneling: disable
```

get system bug-report

Use this command to get information about configuration related to bug reporting. To configure a custom email relay for sending problem reports to Fortinet customer support, see config system bug-report on page 89.

Syntax

```
get system bug-report
```

Example output

```
S524DF4K15000024 # get system bug-report

auth                : no
mailto              : fortiswitch@fortinet.com
password            : (null)
server              : fortinet.com
username            : bug_report
username-smtp       : bug_report
```

get system certificate

Use this command to display configuration related to central management service:

Syntax

```
get system certificate (ca | crl | local | oscp | remote)
```

Variable	Description
ca	List available CA certificates.
crl	Display the certificate revocation lists available.
local	List available local keys and certificates.
ocsp	Display the OCSP (Online Certificate Status Protocol) server certificate, the action to take when the server is unavailable, and the URL to the OCSP server.
remote	List available remote certificates.

Example output

```
S524DF4K15000024 # get system certificate ca
== [ Fortinet_CA ]
name: Fortinet_CA
== [ Fortinet_CA2 ]
name: Fortinet_CA2
== [ Entrust_802.1x_CA ]
name: Entrust_802.1x_CA
== [ Entrust_802.1x_L1K_CA ]
name: Entrust_802.1x_L1K_CA
== [ Entrust_802.1x_G2_CA ]
name: Entrust_802.1x_G2_CA

S524DF4K15000024 # get system certificate crl
== [ 1 ]
name: 1

S524DF4K15000024 # get system certificate local
== [ Fortinet_Factory ]
name: Fortinet_Factory
== [ Fortinet_Firmware ]
name: Fortinet_Firmware
== [ Entrust_802.1x ]
name: Entrust_802.1x

S524DF4K15000024 # get system certificate ocsp
cert                : (null)
unavail-action      : revoke
url                 : (null)

S524DF4K15000024 # get system certificate remote
== [ 1 ]
name: 1
```

get system cmdb status

Use this command to view information about configuration management database (CMDB) on the FortiSwitch.

Syntax

```
get system cmdb status
```

Variable	Description
version	Version of the CMDB software.
owner id	Process identifier of the CMDB server daemon.

Variable	Description
update index	The updated index shows how many changes have been made in the CMDB.
config checksum	The configuration file version used by FortiManager.
last request pid	The last process to access the CMDB.
last request type	Type of the last attempted access of the CMDB.
last request	The number of the last attempted access of the CMDB.

Example output

```
# get system cmdb status
version: 1
owner id: 18
update index: 6070
config checksum: 12879299049430971535
last request pid: 68
last request type: 29
last request: 78
```

get system console

Use this command to get information about the console connection. To configure the console, see config system console on page 94.

Syntax

```
get system console
```

Example output

```
S524DF4K15000024 # get system console

baudrate            : 115200
mode                : line
output              : more
```

get system dns

Use this command to get information about the DNS settings. To configure DNS, see config system dns on page 94.

Syntax

```
get system dns
```

Example output

```
S524DF4K15000024 # get system dns

primary             : 208.91.112.53
secondary           : 208.91.112.52
domain              : (null)
ip6-primary         : ::
ip6-secondary       : ::
dns-cache-limit     : 5000
dns-cache-ttl       : 1800
cache-notfound-responses: disable
source-ip           : 0.0.0.0
```

get system fsw-cloud

Use this command to display the configuration of the FortiSwitch cloud manager. To configure the FortiSwitch cloud manager, see config system fsw-cloud on page 95.

Syntax

```
get system fsw-cloud
```

Example output

```
S524DF4K15000024 # get system fsw-cloud

interval            : 15
name                : fortiswitch-dispatch.forticloud.com
port                : 443
status              : enable
```

get system fsw-cloud-mgr connection-info

Use this command to check your connections to the FortiSwitch cloud manager.

Syntax

```
get system fsw-cloud-mgr connection-info
```

Example output

```
S1D243Z14000027 # get system fsw-cloud-mgr connection-info

Dispatch Service : IP= xx.xxx.xxx.xx
Access Service : IP= xx.xxx.xxx.xxx, Port= 443, Connected on: 2017-10-25 18:03:33
State-Machine : State= FSMGR_STATE_READY, Event= EV_READY_HBEAT_GOOD

Bootstrap Service : hostname= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.com, Port= 8000
Bootstrap State : State= OK, api-ver= v1
```

```
SSL verify Code : ok
SSL Tunnel Uptime : Days: 0 Hours: 20 Mins: 5
SSL Tunnel stats : restart-count= 5, Reason= HTTP Response data error

Stats:
========
Switch Keep Alive Tx/Reply := 2408 / 2408
Manager Keep Alive Rx/Error := 2410 / 0

Socks Req Rx/Last Stream-ID := 10131 / 490
Reset Req Rx/last Stream-ID := 247 / 490
Goaway Req Rx := 0
Unknown Req Rx := 0

Syslog Tx/Err := 199 / 0

Used SOCKS stream-id:
======================
SID SockFd State Description

___ ______ _____ _________________
5 0 DATA SYSLOG DATA
```

get system global

Use this command to get the global settings of your FortiSwitch. To configure global settings, config system global on page 96.

Syntax

```
get system global
```

Example output

```
S524DF4K15000024 # get system global

802.1x-ca-certificate: Entrust_802.1x_CA
802.1x-certificate  : Entrust_802.1x
admin-concurrent    : enable
admin-https-pki-required: disable
admin-https-ssl-versions: tlsv1-1 tlsv1-2
admin-lockout-duration: 60
admin-lockout-threshold: 3
admin-port          : 80
admin-scp           : disable
admin-server-cert   : Fortinet_Firmware
admin-sport         : 443
admin-ssh-grace-time: 120
admin-ssh-port      : 22
admin-ssh-v1        : disable
admin-telnet-port   : 23
admintimeout        : 5
allow-subnet-overlap: disable
```

```
asset-tag           : (null)
cfg-save            : automatic
csr-ca-attribute    : enable
daily-restart       : disable
detect-ip-conflict  : enable
dst                 : enable
gui-lines-per-page  : 50
hostname            : S524DF4K15000024
image-rotation      : disable
kernel-crashlog     : enable
language            : english
ldapconntimeout     : 500
radius-port         : 1812
refresh             : 0
remoteauthtimeout   : 5
revision-backup-on-logout: enable
revision-backup-on-upgrade: enable
strong-crypto       : disable
switch-mgmt-mode    : local
timezone            : (GMT-8:00)Pacific Time(US&Canada).
user-server-cert    : Fortinet_Factory
```

get system info admin ssh

Use this command to display information about the SSH configuration on the FortiSwitch such as:

- the SSH port number
- the interfaces with SSH enabled
- the hostkey DSA fingerprint
- the hostkey RSA fingerprint

Syntax

```
get system info admin ssh
```

Example output

```
# get system info admin ssh
SSH v2 is enabled on port 22
SSH is enabled on the following 1 interfaces:
mgmt
SSH hostkey DSA fingerprint = cd:e1:87:70:bb:f0:9c:7d:e3:7b:73:f7:44:23:a5:99
SSH hostkey RSA fingerprint = c9:5b:49:1d:7c:ba:be:f3:9d:39:33:4d:48:9d:b8:49
```

get system info admin status

Use this command to display administrators that are logged into the FortiSwitch.

Syntax

```
get system info admin status
```

Variable	Description
Index	The order the administrators logged in.
User name	The name of the user account logged in.
Login type	Which interface was used to log in.
From	The IP address this user logged in from.

Example output

```
Index User name Login type From
0 admin CLI ssh(172.20.120.16)
1 admin WEB 172.20.120.16
```

get system interface physical

Use this command to list information about the physical network interfaces.

Syntax

```
get system interface physical
```

Example output

```
S524DF4K15000024 # get system interface physical

== [onboard]
       ==[internal]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: n/a (Duplex: n/a)
                rx : 0 bytes  0 packets
                tx : 8405158 bytes  160742 packets
       ==[mgmt]
                mode: dhcp
                ip: 10.105.19.3 255.255.252.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
                rx : 11558117 bytes  85986 packets
                tx : 7048800 bytes  39380 packet
```

get system link-monitor

Use this command to list information about the physical network interfaces. To configure the link health monitor, see config system link-monitor on page 108.

Syntax

```
get system link-monitor
```

get system ntp

Use this command to get information about the NTP settings. To configure an NTP server, see config system ntp on page 109.

Syntax

```
get system ntp
```

Example output

```
ntpserver:
== [ 1 ]
id: 1
== [ 2 ]
id: 2
ntpsync : enable
source-ip : 0.0.0.0
syncinterval : 1
```

get system password-policy

Use this command to view the password policy. To create a password policy, see config system password-policy on page 110.

Syntax

```
get system password-policy
```

Example output

```
# get system password-policy
status : enable
apply-to : admin-password
minimum-length : 8
min-lower-case-letter: 2
min-upper-case-letter: 2
min-non-alphanumeric: 0
min-number : 2
    change-4-characters : disable
expire-status : disable
```

get system performance firewall statistics

Use this command to display a list of traffic types (such as browsing, email, and DNS) and the number of packets and number of payload bytes accepted by the firewall for each type since the system was restarted.

Syntax

```
get system performance firewall statistics
```

Example output

```
get system performance firewall statistics
getting traffic statistics...
Browsing: 623738 packets, 484357448 bytes
DNS: 5129187383836672 packets, 182703613804544 bytes
E-Mail: 23053606 packets, 2 bytes
FTP: 0 packets, 0 bytes
Gaming: 0 packets, 0 bytes
IM: 0 packets, 0 bytes
Newsgroups: 0 packets, 0 bytes
P2P: 0 packets, 0 bytes
Streaming: 0 packets, 0 bytes
TFTP: 654722117362778112 packets, 674223966126080 bytes
VoIP: 16834455 packets, 10 bytes
Generic TCP: 266287972352 packets, 8521215115264 bytes
Generic UDP: 0 packets, 0 bytes
Generic ICMP: 0 packets, 0 bytes
Generic IP: 0 packets, 0 bytes
```

get system performance status

Use this command to display FortiSwitch CPU usage, memory usage, network usage, sessions, virus, IPS attacks, and system up time.

Syntax

```
get system performance status
```

Example output

```
S524DF4K15000024 # get system performance status

CPU states: 0% user 16% system 0% nice 84% idle
Memory states: 10% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30
minutes
Uptime: 0 days,  22 hours,  5 minutes
```

Variable	Description
CPU states	The percentages of CPU cycles used by user, system, nice and idle categories of processes. These categories are: `user` -CPU usage of normal user-space processes `system` -CPU usage of kernel `nice` - CPU usage of user-space processes having other-than-normal running priority `idle` - Idle CPU cycles Adding user, system, and nice produces the total CPU usage as seen on the CPU widget on the web-based system status dashboard.
Memory states	The percentage of memory used.
Average network usage	The average amount of network traffic in kbps in the last 1, 10 and 30 minutes.
Uptime	How long since the system has been restarted.

get system performance top

Use this command to display the list of processes running on the system (similar to the Linux `top` command).

The following commands are available when **get system performance top** is running:

- Press Q or Ctrl+C to quit.
- Press P to sort the processes by the amount of CPU that the processes are using.
- Press M to sort the processes by the amount of memory that the processes are using.

Syntax

```
get system performance top [<delay_int>] <max_lines_int>]]
```

Variable	Description
<delay_int>	The delay, in seconds, between updating the process list. The default is 5 seconds.
<max_lines_int>	The maximum number of processes displayed in the output. The default is 20 lines.

```
S524DF4K15000024 # get system performance top

Run Time:  0 days, 22 hours and 13 minutes
0U, 7S, 93I; 1978T, 1684F
newcli           3424      R <     0.1     0.4
```

```
pyfcgid           770      S        0.0      0.7
pyfcgid           898      S        0.0      0.7
pyfcgid           899      S        0.0      0.7
cmdbsvr           610      S        0.0      0.6
httpsd            771      S        0.0      0.6
httpsd           1998      S        0.0      0.5
httpsd            901      S        0.0      0.5
miglogd           773      S        0.0      0.5
initXXXXXXXXXXX     1      S        0.0      0.5
newcli           1040      S <      0.0      0.5
ipconflictd       799      S        0.0      0.5
httpsd            900      S        0.0      0.4
fsmgrd            806      S        0.0      0.4
lldpmedd          800      S        0.0      0.4
eap_proxy         804      S        0.0      0.4
authd             803      S        0.0      0.4
router_launcher   768      S        0.0      0.4
sshd              790      S        0.0      0.4
stpd              795      S        0.0      0.4
```

get system settings

Use this command to get information about equal cost multi-path (ECMP) routing. To configure ECMP routing, see config system settings on page 111.

Syntax

```
get system settings
```

Example output

```
#get system settings
v4-ecmp-mode : source-ip-based
```

get system sflow

Use this command to display the sFlow settings. To configure sFlow, see config system sflow on page 112.

Syntax

```
get system sflow
```

Example output

```
S524DF4K15000024 # get system sflow

collector-ip        : 0.0.0.0
collector-port      : 6343
```

get system snmp sysinfo

Use this command to get information about your system's SNMP settings. To configure the SNMP agent, see config system snmp sysinfo on page 115.

Syntax

```
get system snmp sysinfo
```

Example output

```
S524DF4K15000024 # get system snmp sysinfo

contact-info        : (null)
description         : (null)
engine-id           : (null)
location            : (null)
status              : disable
trap-high-cpu-threshold: 80
trap-log-full-threshold: 90
trap-low-memory-threshold: 80
trap-temp-alarm-threshold: 60
trap-temp-warning-threshold: 50
```

get system source-ip status

Use this command to list defined source-IPs.

Syntax

```
get system source-ip status
```

Example output

```
# get sys source-ip status
The following services force their communication to use
a specific source IP address:

service=NTP source-ip=172.18.19.101
service=DNS source-ip=172.18.19.101
vdom=root service=RADIUS name=server-pc25 source-ip=10.1.100.101
vdom=root service=TACACS+ name=tac_plus_pc25 source-ip=10.1.100.101
vdom=root service=FSAE name=pc26 source-ip=172.18.19.101
vdom=V1 service=RADIUS name=pc25-Radius source-ip=172.16.200.101
vdom=V1 service=TACACS+ name=pc25-tacacs+ source-ip=172.16.200.101
vdom=V1 service=FSAE name=pc16 source-ip=172.16.200.101
```

get system startup-error-log

Use this command to display information about system startup errors. This command only displays information if an error occurs when the system starts up.

Syntax

```
get system startup-error-log
```

get system status

Use this command to display FortiSwitch status information including:

- firmware version, build number, and branch point
- serial number
- host name
- system time and date and related settings

Syntax

```
get system status
```

Example output

```
S524DF4K15000024 # get system status

Version: FortiSwitch-524D-FPOE v3.6.2,build0382,170829 (GA)
Serial-Number: S524DF4K15000024
BIOS version: 04000013
System Part-Number: P18045-04
Burn in MAC: 08:5b:0e:f1:95:e4
Hostname: S524DF4K15000024
Distribution: International
Branch point: 382
System time: Tue Sep 12 16:16:40 2017
```

get test

Use this command to display information about applications on this FortiSwitch:

Syntax

```
get test {dnsproxy | fpmd | radiusd | sflowd | snmpd} <test_level_int>
```

Variable	Description
{dnsproxy | fpmd | radiusd | sflowd | snmpd}	Set the application to be tested. Tests can be run on the following applications: • `dnsproxy` — DNS proxy • `fpmd` — FPM daemon • `radiusd`— RADIUS daemon • `sflowd` — sFlow daemon • `snmpd`— SNMP daemon
<test_level_int>	Set the level for the test.

Example output

```
S524DF4K15000024 # get test fpmd 1
ROUTE_V4_ADD                    : 9
INTF_V4_ADDR_ADD                : 14
ROUTE_V4_MGMT_FWD_DISABLED      : 4
ROUTE_ADD_INVALID_FAMILY        : 3
ROUTE_ADD_INET127               : 1

S524DF4K15000024 # get test sflowd 1
cmf sflow collector:0.0.0.0:[6343]
sflowd collector:0.0.0.0:[6343]
```

get user group

Use this command to list all user groups. To add a user group, see config user group on page 117.

Syntax

```
get user group
```

Example output

```
S524DF4K15000024 # get user group
== [ group1 ]
name: group1
== [ radgroup ]
name: radgroup
```

get user ldap

Use this command to list LDAP users. To add an LDAP user, see config user ldap on page 119.

Syntax

```
get user ldap
```

get user local

Use this command to list local users. To add a local user, see config user local on page 120.

Syntax

```
get user local
```

Example output

```
S524DF4K15000024 # get user local

== [ user1 ]
name: user1
```

get user radius

Use this command to list RADIUS users. To add a RADIUS user, see config user radius on page 122.

Syntax

```
get user radius
```

Example output

```
S524DF4K15000024 # get user radius

== [ serve2 ]
name: serve2
== [ radone ]
name: radone
```

get user setting

Use this command to get information about all the system's user settings.

Syntax

```
get user setting
```

Example output

```
S524DF4K15000024 # get user setting

auth-blackout-time  : 0
```

```
auth-cert           : (null)
auth-http-basic     : disable
auth-invalid-max    : 5
auth-multi-group    : enable
auth-ports:
       == [ 1 ]
       id: 1
auth-secure-http    : disable
auth-timeout        : 5
auth-timeout-type   : idle-timeout
auth-type           : http https ftp telnet
```

get user tacacs+

Use this command to get information about tacacs+ users.

Syntax

```
get user tacacs+
```

Example output

```
S524DF4K15000024 # get user tacacs+

== [ tacserver ]
name: tacserver
```

Copyright© (Undefined variable: FortinetVariables.Copyright Year) Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.