



# CLI Reference

FortiSwitchOS 7.4.9



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



January 23, 2026

FortiSwitchOS 7.4.9 CLI Reference

11-749-1247436-20260123

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>15</b>
<b>Introduction</b> .....	<b>16</b>
FortiSwitch models .....	16
How this guide is organized .....	16
Typographical conventions .....	16
CLI command syntax conventions .....	17
Entering configuration data .....	18
Entering text strings (names) .....	19
Entering numeric values .....	19
<b>config</b> .....	<b>21</b>
config log .....	21
config log custom-field .....	21
config log disk filter .....	22
config log disk setting .....	23
config log eventfilter .....	24
config log gui .....	24
config log memory filter .....	25
config log memory global-setting .....	26
config log memory setting .....	26
config log {syslogd   syslogd2   syslogd3} filter .....	27
config log {syslogd   syslogd2   syslogd3} setting .....	28
config router .....	30
config router access-list .....	30
config router access-list6 .....	31
config router aspath-list .....	32
config router bgp .....	33
config router community-list .....	50
config router isis .....	51
config router key-chain .....	57
config router multicast .....	58
config router multicast-flow .....	59
config router ospf .....	60
config router ospf6 .....	68
config router policy .....	72
config router prefix-list .....	74
config router prefix-list6 .....	75
config router rip .....	76
config router ripng .....	80
config router route-map .....	83
config router setting .....	86
config router static .....	87
config router static6 .....	89
config router vrf .....	90
config switch .....	91
config switch acl 802-1X .....	92

config switch acl egress	94
config switch acl ingress	95
config switch acl policer	99
config switch acl prelookup	100
config switch acl service custom	101
config switch acl settings	103
config switch auto-isl-port-group	103
config switch auto-network	104
config switch global	105
config switch hsr ring	113
config switch hsr settings	114
config switch igmp-snooping globals	115
config switch interface	116
config switch ip-mac-binding	127
config switch ip-source-guard	128
config switch lldp profile	129
config switch lldp settings	134
config switch macsec profile	135
config switch mirror	138
config switch mld-snooping globals	142
config switch mrp profile	142
config switch mrp settings	143
config switch network-monitor directed	144
config switch network-monitor settings	145
config switch phy-mode	146
config switch physical-port	148
config switch prp channel	153
config switch prp settings	154
config switch ptp settings	155
config switch qos dot1p-map	156
config switch qos ip-dscp-map	157
config switch qos qos-policy	158
config switch quarantine	161
config switch rguard-policy	161
config switch security-feature	163
config switch static-mac	166
config switch storm-control	167
config switch stp instance	167
config switch stp settings	169
config switch trunk	170
config switch virtual-port	173
config switch virtual-wire	174
config switch vlan	174
config switch vlan-tpid	182
config switch-controller global	183
config system	184
config system accprofile	185
config system admin	187
config system alias command	189

config system alias group .....	194
config system arp-table .....	195
config system automation-action .....	195
config system automation-stitch .....	198
config system automation-trigger .....	199
config system bluetooth .....	201
config system bug-report .....	201
config system certificate ca .....	202
config system certificate crl .....	203
config system certificate local .....	204
config system certificate ocsf .....	205
config system certificate remote .....	206
config system console .....	206
config system dhcp server .....	207
config system dns .....	213
config system fln-cloud .....	214
config system flow-export .....	215
config system global .....	218
config system interface .....	225
config system ipv6-neighbor-cache .....	238
config system link-monitor .....	239
config system location .....	240
config system ntp .....	244
config system password-policy .....	245
config system ptp interface-policy .....	247
config system ptp profile .....	247
config system schedule group .....	250
config system schedule onetime .....	251
config system schedule recurring .....	251
config system settings .....	252
config system sflow .....	253
config system sniffer-profile .....	254
config system snmp community .....	255
config system snmp sysinfo .....	257
config system snmp user .....	259
config system vxlan .....	261
config system web .....	263
config user .....	264
config user group .....	264
config user ldap .....	266
config user local .....	268
config user peer .....	269
config user peergrp .....	270
config user radius .....	270
config user setting .....	274
config user tacacs+ .....	276
<b>diagnose .....</b>	<b>277</b>
diagnose automation test .....	280
diagnose bpdu-guard display status .....	280

diagnose certificate all .....	281
diagnose certificate ca .....	283
diagnose certificate local .....	284
diagnose certificate remote .....	284
diagnose debug application .....	285
diagnose debug authd .....	287
diagnose debug bfd .....	288
diagnose debug bgp .....	288
diagnose debug cli .....	288
diagnose debug config-error-log .....	288
diagnose debug console .....	289
diagnose debug crashlog .....	289
diagnose debug disable .....	290
diagnose debug enable .....	291
diagnose debug info .....	291
diagnose debug isis .....	291
diagnose debug kernel level .....	291
diagnose debug ospf .....	292
diagnose debug ospf6 .....	292
diagnose debug packet_test .....	292
diagnose debug pbr .....	293
diagnose debug pim .....	293
diagnose debug port-mac .....	293
diagnose debug report .....	294
diagnose debug reset .....	295
diagnose debug rip .....	295
diagnose debug ripng .....	296
diagnose debug static .....	296
diagnose debug unit_test .....	296
diagnose debug zebra .....	296
diagnose firewall ip clear-counter .....	296
diagnose firewall ip show .....	297
diagnose firewall ipv6 clear-counter .....	297
diagnose firewall ipv6 show .....	297
diagnose flapguard status .....	297
diagnose hardware .....	299
diagnose ip address .....	302
diagnose ip arp .....	303
diagnose ip route .....	303
diagnose ip router {bfd   bgp   isis   ospf   ospf6   pim   pbr   rip   ripng   static   zebra} .....	305
diagnose ip router command .....	306
diagnose ip router fwd .....	306
diagnose ip router process show .....	307
diagnose ip router terminal-monitor .....	308

diagnose ip rtcache list .....	308
diagnose ip rules list .....	308
diagnose ip tcp .....	308
diagnose ip udp .....	309
diagnose ipv6 address .....	310
diagnose ipv6 devconf .....	311
diagnose ipv6 ipv6-tunnel .....	312
diagnose ipv6 neighbor-cache .....	312
diagnose ipv6 route .....	313
diagnose ipv6 sit-tunnel .....	314
diagnose log alertconsole .....	314
diagnose loop-guard status .....	316
diagnose option82-mapping relay .....	317
diagnose option82-mapping snooping .....	317
diagnose settings .....	317
diagnose sniffer packet .....	318
diagnose snmp .....	320
diagnose stp instance list .....	320
diagnose stp mst-config list .....	322
diagnose stp rapid-pvst-port .....	323
diagnose stp vlan list .....	323
diagnose switch 802-1x status .....	325
diagnose switch 802-1x status-dacl .....	326
diagnose switch acl counter .....	326
diagnose switch acl hw-entry-index .....	328
diagnose switch acl schedule .....	328
diagnose switch arp-inspection stats clear .....	329
diagnose switch cpuq .....	329
diagnose switch egress list .....	330
diagnose switch fortilink-auth statistics .....	331
diagnose switch fortilink-auth status .....	331
diagnose switch hsr .....	331
diagnose switch ip-mac-binding entry .....	331
diagnose switch ip-source-guard hardware entry filter .....	332
diagnose switch ip-source-guard hardware entry list .....	332
diagnose switch mac-address .....	333
diagnose switch macsec statistics .....	334
diagnose switch macsec status .....	335
diagnose switch managed-switch .....	335
diagnose switch mclag .....	335
diagnose switch mirror auto-config .....	336
diagnose switch mirror hardware status .....	337
diagnose switch modules .....	338
diagnose switch mrp .....	339

diagnose switch network-monitor .....	339
diagnose switch pdu-counters .....	340
diagnose switch physical-ports cable-diag .....	341
diagnose switch physical-ports datarate .....	342
diagnose switch physical-ports eee-status .....	342
diagnose switch physical-ports hw-counter .....	343
diagnose switch physical-ports io-stats .....	344
diagnose switch physical-ports led-flash .....	345
diagnose switch physical-ports linerate .....	345
diagnose switch physical-ports list .....	345
diagnose switch physical-ports mapping .....	346
diagnose switch physical-ports mdix-status .....	347
diagnose switch physical-ports port-stats .....	347
diagnose switch physical-ports qos-rates .....	348
diagnose switch physical-ports qos-stats .....	350
diagnose switch physical-ports queue-bandwidth-setting .....	351
diagnose switch physical-ports set-counter-revert .....	351
diagnose switch physical-ports set-counter-zero .....	352
diagnose switch physical-ports split-status .....	352
diagnose switch physical-ports stats .....	352
diagnose switch physical-ports summary .....	353
diagnose switch physical-ports virtual-wire list .....	354
diagnose switch poe status .....	354
diagnose switch prp .....	355
diagnose switch ptp port add-link-delay .....	355
diagnose switch ptp port get-link-delay .....	355
diagnose switch qnq dtag-cfg .....	356
diagnose switch storm-control .....	356
diagnose switch trunk list .....	357
diagnose switch trunk summary .....	359
diagnose switch vlan .....	360
diagnose switch vlan-mapping egress hardware-entry .....	362
diagnose switch vlan-mapping ingress hardware-entry .....	362
diagnose switch vxlan arp-nd-cache .....	362
diagnose switch vxlan mac-address list .....	363
diagnose switch vxlan vp-info .....	363
diagnose sys checkused .....	363
diagnose sys cpuset .....	364
diagnose sys dayst-info .....	364
diagnose sys fan status .....	364
diagnose sys flan-cloud-mgr .....	365
diagnose sys flash .....	365
diagnose sys flow-export .....	366
diagnose sys kill .....	366

diagnose sys link-monitor .....	366
diagnose sys mpstat .....	367
diagnose sys ntp status .....	367
diagnose sys pcb temp .....	367
diagnose sys permission list .....	368
diagnose sys permission list-by-accprofile .....	368
diagnose sys permission list-cli .....	369
diagnose sys process .....	369
diagnose sys psu status .....	370
diagnose sys remote assistance .....	370
diagnose sys sniffer-profile .....	371
diagnose sys soc temp .....	371
diagnose sys top .....	372
diagnose sys vlan list .....	373
diagnose test application .....	373
diagnose test authserver .....	374
diagnose user radius coa .....	375
<b>execute .....</b>	<b>376</b>
execute 802-1x clear mac .....	378
execute 802-1x clear interface .....	378
execute 802-1x dacl-clr-stat .....	379
execute 802-1x dacl-reinstall .....	379
execute acl clear-counter .....	379
execute acl key-compaction .....	380
execute alias configure .....	380
execute alias script .....	382
execute backup config .....	382
execute backup full-config .....	383
execute backup memory .....	384
execute batch .....	385
execute bpdu-guard .....	386
execute cfg reload .....	387
execute cfg save .....	387
execute clear switch igmp-snooping .....	388
execute clear switch mld-snooping .....	389
execute clear system arp table .....	389
execute cli check-template-status .....	390
execute cli status-msg-only .....	390
execute date .....	390
execute dhcp lease-clear .....	391
execute dhcp lease-list .....	391
execute dhcp-snooping .....	392
execute disconnect-admin-session .....	392
execute factoryreset .....	393

execute factoryresetfull .....	393
execute flapguard reset .....	393
execute fortilink-auth clearstat .....	394
execute fortilink-auth reauth .....	394
execute fortilink-auth reset .....	394
execute interface dhcpclient-renew .....	394
execute interface dhcp6client-renew .....	395
execute interface pppoe-reconnect .....	395
execute license add .....	395
execute license enhanced-debugging .....	395
execute license status .....	396
execute log delete .....	396
execute log delete-all .....	397
execute log display .....	397
execute log filter .....	397
execute log-report reset .....	398
execute loop-guard reset .....	399
execute mac clear .....	399
execute mac-limit-violation reset .....	399
execute macsec clearstat physical-port .....	400
execute macsec reset physical-port .....	400
execute macsec toggle physical-port .....	401
execute mtracroute .....	401
execute ping .....	402
execute ping-options .....	403
execute ping6 .....	404
execute ping6-options .....	405
execute poe-reset .....	406
execute reboot .....	407
execute rest list .....	407
execute rest login .....	408
execute rest logout .....	408
execute rest run .....	409
execute rest schema .....	411
execute restore bios .....	412
execute restore config .....	412
execute restore image .....	413
execute restore license .....	414
execute revision .....	415
execute router clear bgp .....	416
execute router clear evpn dup-addr .....	417
execute router clear ospf .....	417
execute router tech-support .....	417
execute set-next-reboot .....	418

execute shutdown .....	418
execute source-guard-violation reset .....	419
execute ssh .....	419
execute ssh-regen-keys .....	420
execute stage .....	420
execute sticky-mac .....	421
execute switch-controller clear-nac-mac-cache .....	421
execute switch-controller delete-nac-mac-cache .....	421
execute switch-controller get-conn-status .....	422
execute switch-controller get-nac-mac-cache .....	422
execute system admin account-convert-sha1 .....	423
execute system admin account-convert-sha256 .....	423
execute system certificate ca .....	424
execute system certificate crl import auto .....	424
execute system certificate local export tftp .....	425
execute system certificate local generate ec .....	425
execute system certificate local generate rsa .....	426
execute system certificate local import tftp .....	427
execute system certificate remote .....	427
execute system sniffer-profile delete-capture .....	428
execute system sniffer-profile pause .....	428
execute system sniffer-profile start .....	429
execute system sniffer-profile stop .....	429
execute system sniffer-profile upload .....	430
execute telnet .....	430
execute time .....	431
execute traceroute .....	431
execute tracert6 .....	432
execute upload config .....	433
execute verify image .....	433
execute wake-on-lan .....	434
<b>get .....</b>	<b>436</b>
get hardware cpu .....	438
get hardware memory .....	439
get hardware status .....	440
get log custom-field .....	440
get log eventfilter .....	441
get log gui .....	442
get log memory .....	442
get log syslogd .....	443
get log syslogd2 .....	444
get log syslogd3 .....	445
get router info bfd neighbor .....	446
get router info bgp .....	446

get router info evpn .....	447
get router info gwdetect .....	448
get router info isis .....	448
get router info kernel .....	449
get router info pbr .....	449
get router info multicast .....	450
get router info ospf .....	451
get router info rip .....	453
get router info routing-table .....	454
get router info vrrp .....	455
get router info6 bfd neighbor .....	456
get router info6 bgp .....	456
get router info6 isis .....	457
get router info6 kernel .....	457
get router info6 ospf .....	458
get router info6 rip .....	459
get router info6 routing-table .....	459
get router info6 vrrp .....	460
get switch acl .....	461
get switch dhcp-snooping .....	462
get switch flapguard settings .....	464
get switch global .....	464
get switch igmp-snooping .....	465
get switch interface .....	466
get switch ip-mac-binding .....	467
get switch ip-source-guard .....	467
get switch ip-source-guard-violations .....	468
get switch lldp .....	468
get switch mac-limit-violations .....	469
get switch mirror status .....	470
get switch mld-snooping .....	471
get switch modules .....	472
get switch network-monitor .....	473
get switch mrp .....	474
get switch phy-mode .....	475
get switch physical-port .....	475
get switch poe inline .....	476
get switch qos .....	477
get switch raguard-policy .....	477
get switch security-feature .....	478
get switch static-mac .....	478
get switch storm-control .....	479
get switch stp instance .....	479
get switch stp settings .....	480

get switch trunk .....	480
get switch virtual-wire .....	481
get switch vlan .....	481
get system accprofile .....	482
get system admin list .....	482
get system admin status .....	483
get system arp .....	484
get system arp-table .....	484
get system bug-report .....	484
get system certificate .....	485
get system cmdb status .....	486
get system console .....	487
get system dns .....	487
get system flan-cloud .....	488
get system flan-cloud-mgr connection-info .....	488
get system flow-export .....	490
get system flow-export-data .....	491
get system global .....	491
get system info admin ssh .....	492
get system info admin status .....	493
get system interface physical .....	493
get system interface vlan .....	494
get system interface vxlan .....	495
get system ipv6-neighbor-cache .....	496
get system link-monitor .....	496
get system location .....	496
get system ntp .....	497
get system password-policy .....	497
get system performance firewall statistics .....	498
get system performance status .....	498
get system performance top .....	499
get system schedule group .....	500
get system schedule onetime .....	500
get system schedule recurring .....	501
get system settings .....	501
get system sflow .....	502
get system sniffer-profile capture .....	502
get system sniffer-profile summary .....	502
get system snmp sysinfo .....	503
get system source-ip status .....	503
get system startup-error-log .....	504
get system status .....	504
get test .....	505
get user group .....	506

---

get user ldap .....	506
get user local .....	506
get user radius .....	507
get user setting .....	507
get user tacacs+ .....	508
<b>sleep .....</b>	<b>509</b>
<b>Appendix: FortiSwitch QoS template .....</b>	<b>510</b>

# Change log

Date	Change Description
January 23, 2026	Initial version for FortiSwitchOS 7.4.9

# 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 sections 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 unit.
- `diagnose`—commands that help with troubleshooting.
- `execute`—commands that perform immediate operations.
- `get`—commands that provide information about FortiSwitch operation.
- `sleep`—command to add a delay in a script.

## Typographical conventions

This document uses the following typographical conventions:

Convention	Example
CLI input	<pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>
CLI output	<pre>FG T-602803030703 # get system setting  comments           : (No default)  opmode             : nat</pre>
Emphasis	HTTP connections are <b>not</b> secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>

Convention	Example
	<BODY><H4>You must authenticate to use this service.</H4>
<b>Hyperlink</b>	Visit the Fortinet Technical Support web site: <a href="https://support.fortinet.com/">https://support.fortinet.com/</a>
<b>Keyboard entry</b>	Type a name for the remote VPN peer or client, such as Central_Office_1.
<b>Publication</b>	For details, see the <a href="#">FortiOS Administration Guide</a> .

## 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.
<xxx_ipv4/mask>	A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, 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.

Convention	Description
<xxx_ipv6/mask>	An IPv6 address and netmask separated by a space.
<xxx_int>	An integer number that is <b>not</b> 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 <code>http://www.fortinet./com/</code> .
Square brackets [ ]	A non-required word or series of words. For example: <code>[verbose {1   2   3}]</code> indicates that you can either omit or type both the <code>verbose</code> word and its accompanying option, such as: <code>verbose 3</code>
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: <code>{enable   disable}</code> indicates that you must enter either <code>enable</code> or <code>disable</code> but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: <code>{http https ping snmp ssh telnet}</code> indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: <code>ping https ssh</code>  <b>NOTE:</b> To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type:  <code>ping https snmp ssh</code>  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).

You can use the “?” in three ways:

- Display brief help during command entry.
- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word and then press the question mark (?) key to display a list of valid word completions or subsequent words.



If you need to enter the “?” character in a case where it is usually not allowed:

1. Press Ctrl+v.
2. Type the “?” character .

## 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 unit:

- [config log on page 21](#)
- [config router on page 30](#)
- [config switch on page 91](#)
- [config switch-controller global on page 183](#)
- [config system on page 184](#)
- [config user on page 264](#)

## 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 on page 21](#)
- [config log disk filter on page 22](#)
- [config log disk setting on page 23](#)
- [config log eventfilter on page 24](#)
- [config log gui on page 24](#)
- [config log memory filter on page 25](#)
- [config log memory global-setting on page 26](#)
- [config log memory setting on page 26](#)
- [config log {syslogd | syslogd2 | syslogd3} filter on page 27](#)
- [config log {syslogd | syslogd2 | syslogd3} setting on page 28](#)

## 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
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
end
```

## config log disk filter

Use this command to define the types of events to log in flash memory.

### Syntax

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

Variable	Description	Default
severity {emergency   alert   critical   error   warning   notification   information   debug}	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. <ul style="list-style-type: none"> <li>emergency – The system is unusable.</li> <li>alert – Immediate action is required.</li> <li>critical – Functionality is affected.</li> <li>error – An erroneous condition exists and functionality is probably affected.</li> <li>warning – Functionality might be affected.</li> <li>notification – Information about normal events.</li> <li>information – General information about system operations.</li> <li>debug – Information used for diagnosing or debugging the system.</li> </ul>	alert

## Example

This example shows how to configure the system to log alert-level and emergency-level events to flash memory:

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

## config log disk setting

Use this command to save event logs in flash memory. This command can be used only on FortiSwitch models that have more than 14 megabytes of flash memory. Up to 15 percent of the data2 partition is used for these logs. By default, event log messages are not saved to flash memory.

### Syntax

```
config log disk setting
  set status {disable | enable}
  set max-log-file-size <integer>
  set diskfull {nolog | overwrite}
  set log-quota <integer>
  set full-first-warning-threshold <20-80>
  set full-second-warning-threshold <50-95>
  set full-final-warning-threshold <70-100>
end
```

Variable	Description	Default
status {disable   enable}	Enter enable to enable logging to flash memory.	disable
max-log-file-size <integer>	Enter the maximum size of the log file, in megabytes, before the log file begins rolling. This value might be inaccurate sometimes. The maximum size of the log file cannot exceed the log-quota value.	1
diskfull {nolog   overwrite}	When the disk is full, set the system to stop logging or to overwrite the oldest log.	overwrite
log-quota <integer>	Enter the number of megabytes allowed for log messages in flash memory.	1
full-first-warning-threshold <20-80>	Enter to configure the first warning before reaching the threshold. You can enter a number between 20 and 80.	75
full-second-warning-threshold <50-95>	Enter to configure the second warning before reaching the threshold. You can enter a number between 50 and 95.	90
full-final-warning-threshold <70-100>	Enter to configure the final warning before reaching the threshold. You can enter a number between 70 and 100.	95

## Example

This example shows how to configure log settings:

```
config log disk setting
  set status enable
  set max-log-file-size 5
  set diskfull nodisk
  set log-quota 5
  set full-first-warning-threshold 50
  set full-second-warning-threshold 75
  set full-final-warning-threshold 90
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. <ul style="list-style-type: none"> <li>emergency – The system is unusable.</li> <li>alert – Immediate action is required.</li> <li>critical – Functionality is affected.</li> <li>error – An erroneous condition exists and functionality is probably affected.</li> <li>warning – Functionality might be affected.</li> <li>notification – Information about normal events.</li> <li>information – General information about system operations.</li> <li>debug – Information used for diagnosing or debugging the system.</li> </ul>	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 <i>enable</i> 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. <ul style="list-style-type: none"> <li>emergency – The system is unusable.</li> <li>alert – Immediate action is required.</li> <li>critical – Functionality is affected.</li> <li>error – An erroneous condition exists and functionality is probably affected.</li> <li>warning – Functionality might be affected.</li> <li>notification – Information about normal events.</li> <li>information – General information about system operations.</li> <li>debug – Information used for diagnosing or debugging the system.</li> </ul>	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 enc-algorithm {disable | high | high-medium | low}
  set certificate <certificate_name>
  set server <server_name>
  set mode {legacy-reliable | reliable | udp}
  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 start logging to system memory.	disable
enc-algorithm {disable   high   high-medium   low}	Set to high, high-medium, or low to specify which encryption algorithm that SSL communication uses for reliable syslog. Set to disable if you do not want to use reliable syslog.	disable
certificate <certificate_name>	Specify the certificate to use to communicate with the syslog server.	No default
server <server_name>	This field is available when status is set to enable. Enter the address of the remote syslog server.	No default
mode {legacy-reliable   reliable   udp}	Set to legacy-reliable to use RFC 3195 for reliable syslog. Set to reliable to use RFC 6587 for reliable syslog. Set to udp to use syslog over UDP.  This field is available when status is set to enable. This field was previously named reliable.	udp
port <port_number>	Set the port number that the server listens to.	514

Variable	Description	Default
	<p>If the mode is set to <code>reliable</code>, the default port is 514. If the mode is set to <code>legacy-reliable</code>, the default port is 601. If the mode is set to <code>udp</code>, the default port is 6514.</p> <p>This field is available when <code>status</code> is set to <code>enable</code>.</p>	
<code>csv {enable   disable}</code>	<p>Enable or disable comma-separated values.</p> <p>This field is available when <code>status</code> is set to <code>enable</code>.</p>	<code>disable</code>
<code>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}</code>	<p>This field is available when <code>status</code> is set to <code>enable</code>. Select the facility for remote syslog:</p> <ul style="list-style-type: none"> <li><code>alert</code>—Use the log alert.</li> <li><code>audit</code>—Use the log audit.</li> <li><code>auth</code>—Use the security/authorization messages.</li> <li><code>authpriv</code>—Use the private security/authorization messages.</li> <li><code>clock</code>—Use the clock daemon.</li> <li><code>cron</code>—Use the clock daemon.</li> <li><code>daemon</code>—Use the system daemon.</li> <li><code>ftp</code>—Use the FTP daemon.</li> <li><code>kernel</code>—Use kernel messages.</li> <li><code>local0</code>—Reserved for local use.</li> <li><code>local1</code>—Reserved for local use.</li> <li><code>local2</code>—Reserved for local use.</li> <li><code>local3</code>—Reserved for local use.</li> <li><code>local4</code>—Reserved for local use.</li> <li><code>local5</code>—Reserved for local use.</li> <li><code>local6</code>—Reserved for local use.</li> <li><code>local7</code>—Reserved for local use.</li> <li><code>lpr</code>—Use the line printer subsystem.</li> <li><code>mail</code>—Use the mail system.</li> <li><code>news</code>—Use the network news subsystem.</li> <li><code>ntp</code>—Use the NTP system.</li> <li><code>syslog</code>—Use messages generated internally by the syslog daemon.</li> <li><code>user</code>—Use random user-level messages.</li> <li><code>uucp</code>—Use the network news subsystem.</li> </ul>	<code>local7</code>
<code>source-ip &lt;IPv4_address&gt;</code>	<p>This field is available when <code>status</code> is set to <code>enable</code>. Enter the source IPv4 address of the syslog.</p>	<code>0.0.0.0</code>

## 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 on page 30](#)
- [config router access-list6 on page 31](#)
- [config router aspath-list on page 32](#)
- [config router bgp on page 33](#)
- [config router community-list on page 50](#)
- [config router isis on page 51](#)
- [config router key-chain on page 57](#)
- [config router multicast on page 58](#)
- [config router multicast-flow on page 59](#)
- [config router ospf on page 60](#)
- [config router ospf6 on page 68](#)
- [config router policy on page 72](#)
- [config router prefix-list on page 74](#)
- [config router prefix-list6 on page 75](#)
- [config router rip on page 76](#)
- [config router ripng on page 80](#)
- [config router route-map on page 83](#)
- [config router setting on page 86](#)
- [config router static on page 87](#)
- [config router static6 on page 89](#)
- [config router vrf on page 90](#)

## config router access-list

Use this command to configure an IPv4 access list. 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_address>
        set exact-match {enable | disable}
      end
    end
  end
```

Variable	Description	Default
<list_str>	Enter the name of the access list. <ul style="list-style-type: none"> <li>If the name is a number in the range of 1-99, you can define Cisco-style wildcard filter criteria with the <code>set wildcard &lt;ip&gt;</code> command.</li> <li>If the name has at least one alphabetic character, you can set the prefix to define regular filter criteria using the <code>set prefix {&lt;xxx.xxx.xxx.xxx&gt; &lt;xxx.xxx.xxx.xxx&gt;   any}</code> command.</li> </ul>	No default
comments <comment_str>	Enter a descriptive comment.	No default
<b>config rule</b>	Configure the access-list rule.	
<rule_int>	The rule identifier.	No default
action {deny   permit}	Set whether the rule allows or denies the IPv4 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. <b>NOTE:</b> The access list name must contain at least one alphabetic character.	any
wildcard <IP_address>	Define Cisco-style wildcard filter criteria. <b>NOTE:</b> The access list name must be a digit in the range of 1-99. Strings are not supported.	No default
exact-match {enable   disable}	Set whether the rule 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
end
```

## config router access-list6

Use this command to configure an IPv6 access list. 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-list6
```

```

edit <name_of_IPv6_access_list>
  set comments <string>
  config rule
    edit <rule_ID>
      set action {deny | permit}
      set prefix6 {<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx> | any}
      set exact-match {enable | disable}
    next
  end
end

```

Variable	Description	Default
<name_of_IPv6_access_list>	Enter the name of the IPv6 access list.	No default
comments <string>	Enter a descriptive comment.	No default
<b>config rule</b>	Configure the IPv6 access-list rule.	
<rule_ID>	The rule identifier.	No default
action {deny   permit}	Set whether the rule allows or denies the IPv6 address.	permit
prefix6 {<xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>   any}	Set the IPv6 prefix to define regular filter criteria, such as any or X:X::X:X/M.	any
exact-match {enable   disable}	Set whether the rule looks for an exact match with the value in the prefix field.	disable

## Example

This example shows how to configure an IPv6 access list:

```

config router access-list6
  edit accesslist1
    set comments "IPv6 access list"
    config rule
      edit 1
        set action permit
        set prefix6 fe80::a5b:eff:fef1:95e5
        set exact-match disable
      next
    end
  end
end

```

## config router aspath-list

Use this command to set or unset Border Gateway Protocol (BGP) AS-path list parameters. By default, BGP uses an ordered list of Autonomous System (AS) numbers to describe the route that a packet takes to reach its destination. A list of these AS numbers is called the AS path. You can filter BGP routes using AS path lists.

Use the `config router aspath-list` command to define an access list that examines the `AS_PATH` attributes of BGP routes to match routes. Each entry in the list defines a rule for matching and selecting routes based on the setting of the `AS_PATH` attribute.

## Syntax

```
config router aspath-list
  edit <AS_path_list_name>
    config rule
      edit <rule_identifier>
        set action {deny | permit}
        set regexp <string>
      end
    end
  end
```

Variable	Description	Default
<AS_path_list_name>	Enter the name of the AS path list.	No default
<b>config rule</b>	Configure the AS path list rule.	
<rule_identifier>	Enter a rule identifier.	No default
action {deny   permit}	Set whether to permit or deny route-based operations, based on the route's <code>AS_PATH</code> attribute.	No default
regexp <string>	Specify the regular expression that will be compared to the <code>AS_PATH</code> attribute (for example, <code>^730\$</code> ). The value is used to match AS numbers. Enclose a complex regular expression value within double-quotation marks.	No default

## config router bgp

Use this command to configure Border Gateway Protocol version-4 (BGP-4) routing parameters. BGP can be used to perform Classless Interdomain Routing (CIDR) and to route traffic between different autonomous systems or domains using an alternative route if a link between a FortiSwitch unit and a BGP peer (such as an ISP router) fails.

## Syntax

```
config router bgp
  set as <MANDATORY_router_AS_number>
  set router-id <MANDATORY_IP_address>
  set keepalive-timer <0-65535>
  set holdtime-timer <0, 3-65535>
  set always-compare-med {disable | enable}
  set bestpath-as-path-ignore {disable | enable}
  set bestpath-cmp-confed-aspash {disable | enable}
  set bestpath-cmp-routerid {disable | enable}
  set bestpath-med-confed {disable | enable}
  set bestpath-med-missing-as-worst {disable | enable}
  set client-to-client-reflection {disable | enable}
  set dampening {disable | enable}
  set dampening-reachability-half-life <1-45>
```

```
    set dampening-reuse <1-20000>
    set dampening-suppress <1-20000>
    set dampening-max-suppress-time <1-255>
set deterministic-med {disable | enable}
set fast-external-failover {disable | enable}
set log-neighbour-changes {disable | enable}
set cluster-id <IP_address>
set confederation-identifier <1-4294967295>
set default-local-preference <0-4294967295>
set scan-time <5-60>
set maximum-paths-ebgp <1-64>
set bestpath-asp-path-multipath-relax {disable | enable}
set maximum-paths-ibgp <1-64>
set distance-external <1-255>
set distance-internal <1-255>
set distance-local <1-255>
set ebgp-requires-policy {disable | enable}
set graceful-stalepath-time <1-3600>
set route-reflector-allow-outbound-policy {disable | enable}
config admin-distance
    edit <identifier>
        set distance <1-255>
        set neighbour-prefix <IPv4_address_netmask>
        set route-list <string>
    end
config admin-distance6
    edit <identifier>
        set distance <1-255>
        set neighbour-prefix <IPv6_address_netmask>
        set route6-list <string>
    end
config aggregate-address
    edit <identifier>
        set as-set {disable | enable}
        set prefix <IPv4_address_netmask>
        set summary-only {disable | enable}
    end
config aggregate-address6
    edit <identifier>
        set prefix <IPv6_address_netmask>
        set summary-only {disable | enable}
    end
config evpn
    set advertise-vni {disable | enable}
    set dup-addr-detection {enable | disable}
    set dup-addr-freeze {disable | permanent | time}
    set dup-addr-freeze-time <30-3600 seconds>
    set dup-addr-max-moves <1-1000>
    set dup-addr-window-time <2-1800 seconds>
    config vni
        edit <VNI_ID>
            set export-rt <ASN:VNI_number or A.B.C.D.VNI_number>
            set import-rt <ASN:VNI_number or A.B.C.D.VNI_number>
            set rd <ASN:VNI_number or A.B.C.D.VNI_number>
        end
    end
config neighbor
```

```
edit "<IPv4_IPv6_address>"
  set advertisement-interval <0-600>
  set allowas-in-enable {disable | enable}
  set allowas-in <1-10>
  set allowas-in-enable6 {disable | enable}
  set allowas-in6 <1-10>
  set attribute-unchanged {as-path | MED | next-hop}
  set attribute-unchanged6 {as-path | MED | next-hop}
  set attribute-unchanged-evpn as-path
  set activate {disable | enable}
  set activate6 {disable | enable}
  set activate-evpn {disable | enable}
  set bfd {disable | enable}
  set capability-dynamic {disable | enable}
  set capability-orf {both | none | receive | send}
  set capability-orf6 {both | none | receive | send}
  set capability-default-originate {disable | enable}
  set capability-default-originate6 {disable | enable}
  set dont-capability-negotiate {disable | enable}
  set ebgp-enforce-multihop {disable | enable}
  set ebgp-multihop-ttl <1-255>
  set ebgp-ttl-security-hops <1-254>
  set next-hop-self {disable | enable}
  set next-hop-self6 {disable | enable}
  set override-capability {disable | enable}
  set passive {disable | enable}
  set remove-private-as {disable | enable}
  set remove-private-as6 {disable | enable}
  set route-reflector-client {disable | enable}
  set route-reflector-client6 {disable | enable}
  set route-reflector-client-evpn {disable | enable}
  set route-server-client {disable | enable}
  set route-server-client6 {disable | enable}
  set shutdown {disable | enable}
  set soft-reconfiguration {disable | enable}
  set soft-reconfiguration6 {disable | enable}
  set soft-reconfiguration-evpn {disable | enable}
  set as-override {disable | enable}
  set as-override6 {disable | enable}
  set strict-capability-match {disable | enable}
  set description <string>
  set distribute-list-in <string>
  set distribute-list-in6 <string>
  set distribute-list-out <string>
  set distribute-list-out6 <string>
  set filter-list-in <string>
  set filter-list-in6 <string>
  set filter-list-out <string>
  set filter-list-out6 <string>
  set interface <interface_name>
  set maximum-prefix <1-4294967295>
  set maximum-prefix6 <1-4294967295>
  set prefix-list-in <string>
  set prefix-list-in6 <string>
  set prefix-list-out <string>
  set prefix-list-out6 <string>
  set remote-as <MANDATORY_1-4294967295>
```

```

    set route-map-in <string>
    set route-map-in6 <string>
    set route-map-in-evpn <string>
    set route-map-out <string>
    set route-map-out6 <string>
    set route-map-out-evpn <string>
    set send-community {both | disable | extended | standard}
    set send-community6 {both | disable | extended | standard}
    set keep-alive-timer <0-65535>
    set holdtime-timer <0, 3-65535>
    set connect-timer <0-65535>
    set unsuppress-map <string>
    set unsuppress-map6 <string>
    set update-source <interface_name>
    set weight <0-65535>
end
config network
  edit <identifier>
    set backdoor {disable | enable}
    set prefix <IPv4_address_netmask>
    set route-map <string>
  end
config network6
  edit <identifier>
    set backdoor {disable | enable}
    set prefix6 <IPv6_address_netmask>
    set route-map <string>
  end
config redistribute {connected | isis | ospf | rip | static}
  set status {disable | enable}
  set route-map <string>
end
config redistribute6 {connected | isis | ospf | rip | static}
  set status {disable | enable}
  set route-map <string>
end
end
end

```

Variable	Description	Default
as <MANDATORY_router_AS_number>	Mandatory. Enter an integer to specify the local autonomous system (AS) number of the FortiSwitch unit. The range is from 1 to 4 294 967 295. A value of 0 disables BGP (disabled by default).	0
router-id <MANDATORY_IP_address>	Mandatory. Specify a fixed identifier for the FortiSwitch unit. A value of 0.0.0.0 is not allowed.	0.0.0.0
keepalive-timer <0-65535>	How often (in seconds) the router sends out keepalive messages to neighbor routers to maintain those sessions.	60

Variable	Description	Default
holdtime-timer <0, 3-65535>	How long (in seconds) the router will wait for a keepalive message before declaring a router offline. A shorter time will find an off-line router faster.	180
always-compare-med {disable   enable}	Always compare Multi-Exit Discriminator (MED).	disable
bestpath-as-path-ignore {disable   enable}	AS_PATH is the BGP attribute that keeps track of each AS that a route advertisement has passed through; it helps prevent routing loops. Enable this option if you want BGP to not use the best AS path. Disable this option if you want BGP to use the best AS path.	disable
bestpath-cmp-confed-aspath {disable   enable}	Enable or disable the comparison of the AS_CONFED_SEQUENCE attribute, which defines an ordered list of AS numbers representing a path from the FortiSwitch unit through autonomous systems within the local confederation.	disable
bestpath-cmp-routerid {disable   enable}	Compare router ID for identical external BGP (EBGP) paths.	disable
bestpath-med-confed {disable   enable}	Compare MED among confederation paths.	disable
bestpath-med-missing-as-worst {disable   enable}	Enable or disable (by default) treating any confederation path with a missing MED metric as the least preferred path.	disable
client-to-client-reflection {disable   enable}	Enable (by default) or disable client-to-client route reflection between internal BGP (IBGP) peers.	enable
dampening {disable   enable}	Enable or disable (by default) route-flap dampening on all BGP routes. A flapping route is unstable and continually transitions down and up (see RFC 2439).	disable
dampening-reachability-half-life <1-45>	If you enable dampening, set the maximum time that a route can be suppressed (in minutes). A route can continue to accumulate penalties while it is suppressed. However, the route cannot be suppressed longer than the maximum time.	15
dampening-reuse <1-20000>	If you enable dampening, set a dampening reuse limit based on the number of accumulated penalties. If the penalty assigned to a flapping route decreases enough to fall below the specified limit, the route is not suppressed.	750

Variable	Description	Default
dampening-suppress <1-20000>	If you enable dampening, set a dampening-suppression limit based on the number of accumulated penalties. A route is suppressed (not advertised) when its penalty exceeds the specified limit.	2000
dampening-max-suppress-time <1-255>	If you enable dampening, set the maximum time that a route can be suppressed. A route can continue to accumulate penalties while it is suppressed. However, the route cannot be suppressed longer than the maximum time.	60
deterministic-med {disable   enable}	Enforce deterministic comparison of MED.	disable
fast-external-failover {disable   enable}	Reset peer BGP session if link goes down.	enable
log-neighbour-changes {disable   enable}	Enable or disable logging of BGP neighbor's changes.	enable
cluster-id <IP_address>	Route reflector cluster ID.	0.0.0.0
confederation-identifier <1-4294967295>	Confederation identifier.	0
default-local-preference <0-4294967295>	Default local preference.	100
scan-time <5-60>	Background scanner interval (seconds).	60
maximum-paths-ebgp <1-64>	Set the maximum number of paths for equal-cost multi-path (ECMP) routing using the External Border Gateway Protocol (EBGP).	1
bestpath-aspath-multipath-relax {disable   enable}	Enable or disable load sharing across routes that are the same length but have different autonomous system (AS) paths.	disable
maximum-paths-ibgp <1-64>	Set the maximum number of paths for equal-cost multi-path (ECMP) routing using the Internal Border Gateway Protocol (IBGP).	1
distance-external <1-255>	Distance for routes external to the AS.	20
distance-internal <1-255>	Distance for routes internal to the AS.	200
distance-local <1-255>	Distance for routes local to the AS.	200
ebgp-requires-policy {disable   enable}	Enable or disable the requirement for an in-and-out policy for eBGP peers. The default setting prevents the BGP router from learning or advertising prefixes from or to its eBGP peers.	enable

Variable	Description	Default
graceful-stalepath-time <1-3600>	Time to hold stale paths of restarting neighbor (sec).	360
route-reflector-allow-outbound-policy	Enable or disable the route reflector to apply a route map to reflected routes.	disable
<b>config admin-distance</b>	Configure IPv4 administrative distance modifications.	
<identifier>	Enter an identifier to set administrative distance modifications for BGP routes.	No default
distance <1-255>	Set the administrative distance to apply.	0
neighbour-prefix <IPv4_address_netmask>	Neighbor address prefix. Enter the class IPv4 address and netmask with correction.	0.0.0.0 0.0.0.0
route-list <string>	The access list of IPv4 routes this distance will be applied to.	No default
<b>config admin-distance6</b>	Configure IPv6 administrative distance modifications.	
<identifier>	Enter an identifier to set administrative distance modifications for BGP routes.	No default
distance <1-255>	Set the administrative distance to apply.	0
neighbour-prefix <IPv6_address_netmask>	Neighbor address prefix. Enter the class IPv6 address and netmask with correction.	::/0
route6-list <string>	The access list of IPv6 routes this distance will be applied to.	No default
<b>config aggregate-address</b>	Configure the table of BGP IPv4 aggregate addresses.	
<identifier>	Enter a BGP aggregate entry in the routing table. When you aggregate routes, routing becomes less precise because path details are not readily available for routing purposes. The aggregate address represents addresses in several autonomous systems. Aggregation reduces the length of the network mask until it masks only the bits that are common to all of the addresses being summarized.	No default
as-set {disable   enable}	Enable or disable the generation of an unordered list of AS numbers to include in the path information.	disable
prefix <IPv4_address_netmask>	Aggregate IPv4 prefix. The prefix 0.0.0.0 0.0.0.0 is not allowed.	No default
summary-only {disable   enable}	Enable or disable filtering more specific routes from updates.	disable

Variable	Description	Default
<b>config aggregate-address6</b>	Configure the table of BGP IPv6 aggregate addresses.	
<identifier>	Enter a BGP aggregate entry in the routing table. When you aggregate routes, routing becomes less precise because path details are not readily available for routing purposes. The aggregate address represents addresses in several autonomous systems. Aggregation reduces the length of the network mask until it masks only the bits that are common to all of the addresses being summarized.	No default
prefix6 <IPv6_address_netmask>	Aggregate IPv6 prefix.	No default
summary-only {disable   enable}	Enable or disable filtering more specific routes from updates.	disable
<b>config evpn</b>	Configure the BGP Ethernet Virtual Private Network (EVPN).	
advertise-vni {disable   enable}	Enable to advertise all of the configured VNIs under the <code>config system vxlan</code> command. Disable to advertise none of the configured VNIs under the <code>config system vxlan</code> command.	disable
dup-addr-detection {enable   disable}	Enable or disable whether duplicate MAC addresses are detected by FortiSwitchOS in a VXLAN-EVPN network. This field is available when <code>advertise-vni</code> is set to enable.	enable
dup-addr-freeze {disable   permanent   time}	Select whether to lock (freeze) duplicate MAC addresses: <ul style="list-style-type: none"> <li><code>disable</code>—Do not lock (freeze) duplicate MAC addresses.</li> <li><code>permanent</code>—Permanently lock (freeze) duplicate MAC addresses.</li> <li><code>time</code>—Lock (freeze) duplicate MAC addresses for the number of seconds specified in the <code>set dup-addr-freeze-time</code> command.</li> </ul> This field is available when <code>advertise-vni</code> is set to enable.	disable
dup-addr-freeze-time <30-3600 seconds>	Set the number of seconds to lock (freeze) duplicate MAC addresses. This field is available when <code>advertise-vni</code> is set to enable and <code>dup-addr-freeze</code> is set to <code>time</code> .	300

Variable	Description	Default
dup-addr-max-moves <1-1000>	Set the maximum number of times that a MAC address can move across the network before it is detected as a duplicate address. This field is available when advertise-vni is set to enable.	5
dup-addr-window-time <2-1800 seconds>	Set the number of seconds during which the number of times a MAC address moves is counted. This field is available when advertise-vni is set to enable.	100
<b>config vni</b>	Configure the BGP VXLAN network identifier (VNI).	
export-rt "<ASN:VNI_number or A.B.C.D.VNI_number>"	Enter a list of export route targets. If you do not provide this information, BGP will select the default values itself.	No default
import-rt "<ASN:VNI_number or A.B.C.D.VNI_number>"	Enter a list of import route targets. If you do not provide this information, BGP will select the default values itself.	No default
rd "<ASN:VNI_number or A.B.C.D.VNI_number>"	Enter the route distinguisher. If you do not provide this information, BGP will select the default values itself.	No default
<b>config neighbor</b>	Configure the BGP neighbor table.	
<IPv4_IPv6_address>	Enter the IPv4 or IPv6 address of the BGP neighbor.	No default
advertisement-interval <0-600>	Set the minimum amount of time (in seconds) that the FortiSwitch unit waits before sending a BGP routing update to the BGP neighbor.	30
allowas-in-enable {disable   enable}	Enable to allow my AS-in-AS path (for IPv4).	disable
allowas-in <1-10>	If you enable allowas-in-enable, set the maximum number of occurrences of my AS numbers allowed (for IPv4).	No default
allowas-in-enable6 {disable   enable}	Enable to allow my AS-in-AS path (for IPv6).	disable
allowas-in6 <1-10>	If you enable allowas-in-enable6, set the maximum number of occurrences of my AS numbers allowed (for IPv6).	No default
attribute-unchanged as-path	Propagate unchanged BGP attributes to the BGP neighbor by advertising unchanged next-hop attributes.	as-path

Variable	Description	Default
attribute-unchanged6 {as-path   MED   next-hop}	<p>Propagate unchanged BGP attributes to the BGP neighbor using one of the following methods (for IPv6):</p> <ul style="list-style-type: none"> <li>To advertise unchanged next-hop attributes, select as-path.</li> <li>To advertise unchanged MULTI_EXIT_DISC attributes, select med.</li> <li>To keep the next-hop attribute as is, select next-hop.</li> <li>An empty set (default) is a supported value.</li> </ul>	No default
attribute-unchanged-evpn {as-path   med   next-hop}	<p>Propagate unchanged BGP attributes to the BGP neighbor using one of the following methods (for EVPN):</p> <ul style="list-style-type: none"> <li>To advertise unchanged next-hop attributes, select as-path.</li> <li>To advertise unchanged MULTI_EXIT_DISC attributes, select med.</li> <li>To keep the next-hop attribute as is, select next-hop.</li> <li>An empty set (default) is a supported value.</li> </ul>	No default
activate {disable   enable}	Enable address family IPv4 for this neighbor.	enable
activate6 {disable   enable}	Enable address family IPv6 for this neighbor.	enable
activate-evpn {disable   enable}	Enable this option to exchange layer-2 VPN information with this neighbor.	disable
bfd {disable   enable}	Enable BFD for this neighbor.	disable
capability-dynamic {disable   enable}	Advertise dynamic capability to this neighbor.	disable
capability-orf {both   none   receive   send}	<p>Enable advertising of Outbound Routing Filter (ORF) prefix-list capability to the BGP neighbor using one of the following methods (for IPv4):</p> <ul style="list-style-type: none"> <li>none: disable the advertising of ORF prefix-list capability.</li> <li>receive: enable receive capability.</li> <li>send: enable send capability.</li> <li>both: enable send and receive capability.</li> </ul>	none
capability-orf6 {both   none   receive   send}	<p>Enable advertising of ORF prefix-list capability to the BGP neighbor using one of the following methods (for IPv6):</p> <ul style="list-style-type: none"> <li>none: disable the advertising of ORF prefix-list capability.</li> <li>receive: enable receive capability.</li> <li>send: enable send capability.</li> <li>both: enable send and receive capability.</li> </ul>	none

Variable	Description	Default
capability-default-originate {disable   enable}	Advertise the default IPv4 route to this neighbor.	disable
capability-default-originate6 {disable   enable}	Advertise the default IPv6 route to this neighbor.	disable
dont-capability-negotiate {disable   enable}	Do not negotiate capabilities with this neighbor.	disable
ebgp-enforce-multihop {disable   enable}	Enable or disable the allowance of multi-hop EBGP neighbors.	disable
ebgp-multihop-ttl <1-255>	If you enable ebgp-enforce-multihop, define a TTL value for BGP packets sent to the BGP neighbor.	255
ebgp-ttl-security-hops <1-254>	If you enable ebgp-enforce-multihop, specify the maximum number of hops to the EBGP peer.	0
next-hop-self {disable   enable}	Enable or disable IPv4 next-hop calculation for this neighbor.	disable
next-hop-self6 {disable   enable}	Enable or disable IPv6 next-hop calculation for this neighbor.	disable
override-capability {disable   enable}	Enable or disable the overriding of the result of the capability negotiation.	disable
passive {disable   enable}	Enable or disable sending of open messages to this neighbor.	disable
remove-private-as {disable   enable}	Enable or disable the removal of the private AS number from the IPv4 outbound updates.	disable
remove-private-as6 {disable   enable}	Enable or disable the removal of the private AS number from the IPv6 outbound updates.	disable
route-reflector-client {disable   enable}	Enable or disable the IPv4 AS route reflector client.	disable
route-reflector-client6 {disable   enable}	Enable or disable the IPv6 AS route reflector client.	disable
route-reflector-client-evpn {disable   enable}	Enable or disable the EVPN AS route reflector client.	disable
route-server-client {disable   enable}	Enable or disable the IPv4 AS route server client.	disable
route-server-client6 {disable   enable}	Enable or disable the IPv6 AS route server client.	disable
shutdown {disable   enable}	Enable or disable the shutting down of this neighbor.	disable
soft-reconfiguration {disable   enable}	Enable or disable the allowance of IPv4 inbound soft reconfiguration.	disable

Variable	Description	Default
soft-reconfiguration6 {disable   enable}	Enable or disable the allowance of IPv6 inbound soft reconfiguration.	disable
soft-reconfiguration-evpn {disable   enable}	Enable or disable the allowance of EVPN inbound soft reconfiguration.	disable
as-override {disable   enable}	Enable or disable the replacement of the peer AS with own AS for IPv4.	disable
as-override6 {disable   enable}	Enable or disable the replacement of the peer AS with own AS for IPv6.	disable
strict-capability-match {disable   enable}	Enable or disable strict capability matching.	disable
description <string>	Enter a description of this neighbor.	No default
distribute-list-in <string>	Limit route updates from the BGP neighbor based on the Network Layer Reachability Information (NLRI) prefixes defined in the specified IPv4 access list. You must create the access list before it can be selected here. See <a href="#">config router access-list on page 30</a> .	No default
distribute-list-in6 <string>	Limit route updates from the BGP neighbor based on the Network Layer Reachability Information (NLRI) prefixes defined in the specified IPv6 access list. You must create the access list before it can be selected here. See <a href="#">config router access-list6 on page 31</a> .	No default
distribute-list-out <string>	Limit route updates to the BGP neighbor based on the NLRI defined in the specified IPv4 access list. You must create the access list before it can be selected here. See <a href="#">config router access-list on page 30</a> .	No default
distribute-list-out6 <string>	Limit route updates to the BGP neighbor based on the NLRI defined in the specified IPv6 access list. You must create the access list before it can be selected here. See <a href="#">config router access-list6 on page 31</a> .	No default
filter-list-in <string>	BGP AS path filter for IPv4 inbound routes. You must create the AS path list before it can be selected here. See <a href="#">config router aspath-list on page 32</a> .	No default

Variable	Description	Default
filter-list-in6 <string>	BGP AS path filter for IPv6 inbound routes. You must create the AS path list before it can be selected here. See <a href="#">config router aspath-list on page 32</a> .	No default
filter-list-out <string>	BGP AS path filter for IPv4 outbound routes. You must create the AS path list before it can be selected here. See <a href="#">config router aspath-list on page 32</a> .	No default
filter-list-out6 <string>	BGP AS path filter for IPv6 outbound routes. You must create the AS path list before it can be selected here. See <a href="#">config router aspath-list on page 32</a> .	No default
interface <interface_name>	Set the interface.	No default
maximum-prefix <1-4294967295>	Enter the maximum number of IPv4 prefixes to accept from this peer.	unset
maximum-prefix6 <1-4294967295>	Enter the maximum number of IPv6 prefixes to accept from this peer.	unset
prefix-list-in <string>	Limit route updates from a BGP neighbor based on the Network Layer Reachability Information (NLRI) in the specified IPv4 prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See <a href="#">config router prefix-list on page 74</a> .	No default
prefix-list-in6 <string>	Limit route updates from a BGP neighbor based on the Network Layer Reachability Information (NLRI) in the specified IPv6 prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See <a href="#">config router prefix-list6 on page 75</a> .	No default
prefix-list-out <string>	Limit route updates to a BGP neighbor based on the NLRI in the specified IPv4 prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See <a href="#">config router prefix-list on page 74</a> .	No default

Variable	Description	Default
prefix-list-out6 <string>	Limit route updates to a BGP neighbor based on the NLRI in the specified IPv6 prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See <a href="#">config router prefix-list6 on page 75</a> .	No default
remote-as <MANDATORY_1-4294967295>	Mandatory. Adds a BGP neighbor to the FortiSwitch configuration and sets the AS number of the neighbor. If the number is identical to the AS number of the FortiSwitch unit, the FortiSwitch unit communicates with the neighbor using internal BGP (IBGP). Otherwise, the neighbor is an external peer, and the FortiSwitch unit uses EBGp to communicate with the neighbor.	0
route-map-in <string>	Limit route updates or change the attributes of route updates from the BGP neighbor according to the specified IPv4 route map. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
route-map-in6 <string>	Limit route updates or change the attributes of route updates from the BGP neighbor according to the specified IPv6 route map. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
route-map-in-evpn <string>	Limit route updates or change the attributes of route updates from the BGP neighbor according to the specified EVPN route map. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
route-map-out <string>	Limit route updates or change the attributes of route updates to the BGP neighbor according to the specified IPv4 route map. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default

Variable	Description	Default
route-map-out6 <string>	Limit route updates or change the attributes of route updates to the BGP neighbor according to the specified IPv6 route map. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
route-map-out-evpn <string>	Limit route updates or change the attributes of route updates to the BGP neighbor according to the specified EVPN route map. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
send-community {both   disable   extended   standard}	Enable sending the COMMUNITY attribute to the BGP neighbor using one of the following methods (for IPv4): <ul style="list-style-type: none"> <li>• standard: advertise standard capabilities</li> <li>• extended: advertise extended capabilities</li> <li>• both: advertise extended and standard capabilities (default)</li> <li>• disable: disable the advertising of the COMMUNITY attribute</li> </ul>	both
send-community6 {both   disable   extended   standard}	Enable sending the COMMUNITY attribute to the BGP neighbor using one of the following methods (for IPv6): <ul style="list-style-type: none"> <li>• standard: advertise standard capabilities</li> <li>• extended: advertise extended capabilities</li> <li>• both: advertise extended and standard capabilities (default)</li> <li>• disable: disable the advertising of the COMMUNITY attribute</li> </ul>	both
keep-alive-timer <0-65535>	How often (in seconds) the router sends out keepalive messages to neighbor routers to maintain those sessions.	No default
holdtime-timer <0, 3-65535>	How long (in seconds) the router will wait for a keepalive message before declaring a router offline. A shorter time will find an off-line router faster.	No default
connect-timer <0-65535>	Interval (in seconds) for connect timer.	No default

Variable	Description	Default
unsuppress-map <string>	Specify the name of the IPv4 route map to selectively unsuppress suppressed routes. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
unsuppress-map6 <string>	Specify the name of the IPv6 route map to selectively unsuppress suppressed routes. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
update-source <interface_name>	Interface to use as source IP/IPv6 address of TCP connections.	No default
weight <0-65535>	Neighbor weight.	No default
<b>config network</b>	Configure the BGP IPv4 network table.	
<identifier>	Enter an identifier.	No default
backdoor {disable   enable}	Enable route as backdoor.	disable
prefix <IPv4_address_netmask>	Set the network IPv4 prefix. Use the class IPv4 address and netmask with correction.	0.0.0.0 0.0.0.0
route-map <string>	Specify the name of the route map. Only the route maps for this protocol are listed. See <a href="#">config router route-map on page 83</a> .	No default
<b>config network6</b>	Configure the BGP IPv6 network table.	
<identifier>	Enter an identifier.	No default
backdoor {disable   enable}	Enable route as backdoor.	disable
prefix <IPv6_address_netmask>	Set the network IPv6 prefix. Use the class IPv6 address and netmask with correction.	No default
route-map <string>	Specify the name of the route map. Only the route maps for this protocol are listed. See <a href="#">config router route-map on page 83</a> .	No default
<b>config redistribute {connected   isis   ospf   rip   static}</b>	Configure the BGP IPv4 redistribute table.	

Variable	Description	Default
status {disable   enable}	You can enable BGP to provide connectivity between connected, static, RIP, and/or OSPF IPv4 routes. BGP redistributes the routes from one protocol to another. When a large internetwork is divided into multiple routing domains, use the subcommand to redistribute routes to the various domains.	disable
route-map <string>	Specify the name of the route map that identifies the routes to redistribute. If a route map is not specified, all routes are redistributed to BGP. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default
<b>config redistribute6 {connected   isis   ospf   rip   static}</b>	Configure the BGP IPv6 redistribute table.	
status {disable   enable}	You can enable BGP to provide connectivity between connected, static, RIP, and/or OSPF IPv6 routes. BGP redistributes the routes from one protocol to another. When a large internetwork is divided into multiple routing domains, use the subcommand to redistribute routes to the various domains.	disable
route-map <string>	Specify the name of the route map that identifies the routes to redistribute. If a route map is not specified, all routes are redistributed to BGP. Only the route maps for this protocol are listed. You must create the route map before it can be selected here. See <a href="#">config router route-map on page 83</a> .	No default

## Example

This example shows how to configure internal BGP routing:

```
config router bgp
  set as 6500
  set router-id 1.2.3.4
  config neighbor
    edit "172.168.111.5"
      set remote-as 6500
    next
  end
  config network
    edit 1
      set prefix 192.168.2.0 255.255.255.0
    next
  end
```

```

    config redistribute "connected"
    end
  end
end

```

## config router community-list

Use this command to identify BGP routes according to their COMMUNITY attributes (see RFC 1997). Each entry in the community list defines a rule for matching and selecting routes based on the setting of the COMMUNITY attribute.

### Syntax

```

config router community-list
  edit <community_list_name>
    set type {expanded | standard}
    config rule
      edit <rule_identifier>
        set action {deny | permit}
        set regexp <regular_expression>
        set match <community_number | internet | local-AS | no-advertise | no-export>
      end
    end
  end
end

```

Variable	Description	Default
<community_list_name>	Enter a name for the community list. <b>NOTE:</b> If the community list name is a number in the range of 1-99, the type is set to standard by default. If the community list name is a number greater than 99, the type is set to expanded by default.	No default
type {expanded   standard}	Specify the type of community to match. <b>NOTE:</b> This field is valid only when the community list name is not numeric.	standard
<b>config rule</b>	Configure the community list rule.	
<rule_identifier>	Enter a rule identifier.	No default
action {deny   permit}	Permit or deny route-based operations, based on the route's COMMUNITY attribute.	No default
regexp <regular_expression>	If you select an expanded community, specify an ordered list of COMMUNITY attributes as a regular expression. The value or values are used to match a community. Enclose a complex regular expression value within double-quotation marks.	No default
match <community_number   internet   local-AS   no-advertise   no-export>	If you select a standard community, specify the criteria for matching a reserved community: <ul style="list-style-type: none"> <li>Use decimal notation to match one or more COMMUNITY attributes having the syntax AA:NN, where AA represents an AS, and NN is the community identifier. Delimit complex</li> </ul>	No default

Variable	Description	Default
	<p>expressions with double-quotation marks (for example, "123:234 345:456").</p> <ul style="list-style-type: none"> <li>To match all routes in the Internet community, type <code>internet</code>.</li> <li>To match all routes in the LOCAL_AS community, type <code>local-AS</code>. Matched routes are not advertised locally.</li> <li>To select all routes in the NO_ADVERTISE community, type <code>no-advertise</code>. Matched routes are not advertised.</li> <li>To select all routes in the NO_EXPORT community, type <code>no-export</code>. Matched routes are not advertised to EBGp peers. If a confederation is configured, the routes are advertised within the confederation.</li> </ul>	

## config router isis

Intermediate System to Intermediate System Protocol (IS-IS) allows routing of ISO's OSI protocol stack Connectionless Network Service (CLNS). IS-IS is an Interior Gateway Protocol (IGP) that is not intended to be used between Autonomous Systems (AS).

### Syntax

```
config router isis
  set auth-keychain-area <string>
  set auth-keychain-domain <string>
  set auth-mode-area {md5 | password}
  set auth-mode-domain {md5 | password}
  set auth-password-area <password>
  set auth-password-domain <password>
  set auth-sendonly-area {enable | disable}
  set auth-sendonly-domain {enable | disable}
  set default-information-level {level-1 | level-1-2 | level-2}
  set default-information-level6 {level-1 | level-1-2 | level-2}
  set default-information-metric <0-4261412864>
  set default-information-metric6 <0-4261412864>
  set default-information-originate {always | disable | enable}
  set default-information-originate6 {always | disable | enable}
  set ignore-attached-bit {disable | enable}
  set is-type {level-1 | level-1-2 | level-2-only}
  set log-neighbour-changes {disable | enable}
  set lsp-gen-interval-l1 <1-120>
  set lsp-gen-interval-l2 <1-120>
  set lsp-refresh-interval <1-65535>
  set max-lsp-lifetime <350-65535>
  set metric-style {narrow | transition | wide}
  set overload-bit {disable | enable}
  set redistribute-l1 {disable | enable}
  set redistribute-l1-list <string>
  set redistribute6-l1 {disable | enable}
  set redistribute6-l1-list <string>
  set router-id <IP_address>
```

```
set spf-interval-exp-l1 <1-120>
set spf-interval-exp-l2 <1-120>
config interface
  edit <IS-IS interface name>
    set auth-keychain-hello <string>
    set auth-mode-hello {md5 | password}
    set auth-password-hello <password>
    set bfd {enable | disable}
    set bfd6 {enable | disable}
    set circuit-type {level-1 | level-1-2 | level-2}
    set csnp-interval-l1 <1-65535 seconds>
    set csnp-interval-l2 <1-65535 seconds>
    set hello-interval-l1 <1-65535 seconds; 0 to use 1-second hold time>
    set hello-interval-l2 <1-65535 seconds; 0 to use 1-second hold time>
    set hello-multiplier-l1 <2-100>
    set hello-multiplier-l2 <2-100>
    set hello-padding {disable | enable}
    set metric-l1 <1-63>
    set metric-l2 <1-63>
    set passive {disable | enable}
    set priority-l1 <0-127>
    set priority-l2 <0-127>
    set status {disable | enable}
    set status6 {disable | enable}
    set wide-metric-l1 <1-16777214>
    set wide-metric-l2 <1-16777214>
  end
config net
  edit <1-63>
    set <IS-IS net xx.xxxx. ... .xxxx.xx>
  end
config redistribute {bgp | connected | ospf | rip | static}
  set status {disable | enable}
  set metric <0-4261412864>
  set metric-type {external | internal}
  set level {level-1 | level-1-2 | level-2}
  set routemap <string>
end
config redistribute6 {bgp6 | connected | ospf6 | ripng | static}
  set status {disable | enable}
  set metric <0-4261412864>
  set level {level-1 | level-1-2 | level-2}
  set routemap <string>
end
config summary-address
  edit <summary address entry identifier>
    set level {level-1 | level-1-2 | level-2}
    set prefix <IPv4 address and netmask>
  end
config summary-address6
  edit <summary address entry identifier>
    set level {level-1 | level-1-2 | level-2}
    set prefix6 <IPv6 address and netmask>
  end
end
```

Variable	Description	Default
auth-keychain-area <string>	IS-IS area (level-1) authentication key chain. This command is applicable when the area's authentication mode is md5.	No default
auth-keychain-domain <string>	IS-IS domain (level-2) authentication key-chain. This command is applicable when domain's auth mode is md5.	No default
auth-mode-area {md5   password}	IS-IS area (level-1) authentication mode.	password
auth-mode-domain {md5   password}	IS-IS domain (level-2) authentication mode.	password
auth-password-area <password>	IS-IS area (level-1) authentication password. This command is applicable when area's authentication mode is password.	No default
auth-password-domain <password>	IS-IS domain (level-2) authentication password. This command is applicable when domain's authentication mode is password.	No default
auth-sendonly-area {enable   disable}	IS-IS area (level-1) authentication send-only.	disable
auth-sendonly-domain {enable   disable}	IS-IS domain (level-2) authentication send-only.	disable
default-information-level {level-1   level-1-2   level-2}	Distribute default IPv4 route into level's link-state packet (LSP).	level-2
default-information-level6 {level-1   level-1-2   level-2}	Distribute default IPv6 route into level's LSP.	level-2
default-information-metric <0-4261412864>	Default IPv4 information metric.	10
default-information-metric6 <0-4261412864>	Default IPv6 information metric.	10
default-information-originate {always   disable   enable}	Enable or disable the generation of an IPv4 default route.	disable
default-information-originate6 {always   disable   enable}	Enable or disable the generation of an IPv6 default route.	disable
ignore-attached-bit {disable   enable}	Ignore attached bit on incoming level-1 LSP.	disable
is-type {level-1   level-1-2   level-2-only}	Set the IS-IS level to use: <ul style="list-style-type: none"> <li>level-1: intra-area</li> <li>level-1-2: both intra-area and inter-area</li> <li>level-2-only: inter-area</li> </ul>	level-1-2
log-neighbour-changes {disable   enable}	Enable logging of IS-IS neighbor's changes	enable
lsp-gen-interval-l1 <1-120>	Minimum interval for level-1 LSP regenerating.	1

Variable	Description	Default
lsp-gen-interval-l2 <1-120>	Minimum interval for level-2 LSP regenerating.	1
lsp-refresh-interval <1-65535>	LSP refresh time in seconds.	900
max-lsp-lifetime <350-65535>	Maximum LSP lifetime in seconds.	1200
metric-style {narrow   transition   wide}	Use old-style (ISO 10589) or new-style packet formats. <ul style="list-style-type: none"> <li>narrow: Use the old style of TLVs with narrow metric (default)</li> <li>transition: Send and accept both styles of TLVs during the transition.</li> <li>wide: Use the new style of TLVs to carry a wider metric.</li> </ul>	narrow
overload-bit {disable   enable}	Signal other routers not to use this bit in shortest-path-first (SPF).	disable
redistribute-l1 {disable   enable}	Redistribute level-1 IPv4 routes into level 2.	enable
redistribute-l1-list <string>	Access-list for redistributing level-1 IPv4 routes to level 2.	No default
redistribute6-l1 {disable   enable}	Redistribute level-1 IPv6 routes into level 2.	enable
redistribute6-l1-list <string>	Access-list for redistributing level-1 IPv6 routes to level 2.	No default
router-id <IP_address>	Router identifier.	0.0.0.0
spf-interval-exp-l1 <1-120>	Level-1 SPF minimum calculation delay in seconds.	1
spf-interval-exp-l2 <1-120>	Level-2 SPF minimum calculation delay in seconds.	1
<b>config interface</b>	Configure the IS-IS interface.	
<IS-IS interface name>	Select the IS-IS interface name to configure.	No default
auth-keychain-hello <string>	Hello protocol data unit (PDU) authentication key chain. This command is applicable when the hello packet's authentication mode is md5.	No default
auth-mode-hello {md5   password}	Hello PDU authentication mode.	password
auth-password-hello <password>	Hello PDU authentication password. This command is applicable when hello's authentication mode is password.	No default
bfd {enable   disable}	Enable or disable bidirectional forwarding detection (BFD) for IPv4 traffic.	disable
bfd6 {enable   disable}	Enable or disable BFD for IPv6 traffic.	disable
circuit-type {level-1   level-1-2   level-2}	Set the IS-IS circuit type to use for this interface: <ul style="list-style-type: none"> <li>level-1: intra-area</li> <li>level-1-2: both intra-area and inter-area</li> <li>level-2-only: inter-area</li> </ul>	level-1-2
csnp-interval-l1 <1-65535>	Level-1 complete sequence number PDU (CSNP) interval, in number of seconds.	10

Variable	Description	Default
csnp-interval-l2 <1-6553>	Level-2 CSNP interval, in number of seconds.	10
hello-interval-l1 <1-65535>	Level-1 hello packet interval, in number of seconds. Use 0 for a 1-second hold time.	10
hello-interval-l2 <1-65535>	Level-2 hello packet interval, in number of seconds. Use 0 for a 1-second hold time.	10
hello-multiplier-l1 <2-100>	Level-1 multiplier for hello packet holding time.	3
hello-multiplier-l2 <2-100>	Level-2 multiplier for hello packet holding time.	3
hello-padding {disable   enable}	Enable padding to IS-IS hello packets.	enable
metric-l1 <1-63>	Level-1 metric for interface.	10
metric-l2 <1-63>	Level-2 metric for interface.	10
passive {disable   enable}	Set this interface as passive.	disable
priority-l1 <0-127>	Level-1 priority.	64
priority-l2 <0-127>	Level-2 priority.	64
status {disable   enable}	Enable or disable the interface for IS-IS for IPv4 traffic.	enable
status6 {disable   enable}	Enable or disable the interface for IS-IS for IPv6 traffic.	enable
wide-metric-l1 <1-16777214>	Level-1 wide metric for interface.	10
wide-metric-l2 <1-16777214>	Level-2 wide metric for interface.	10
<b>config net</b>	Configure the IS-IS network.	
<1-63>	An integer identifier.	No default
<IS-IS net xx.xxxx. ....xxxx.xx>	Set the IS-IS network.	No default
<b>config redistribute {bgp   connected   ospf   rip   static}</b>	Configure the IS-IS redistribute IPv4 protocols.	
status {disable   enable}	Enable or disable the redistribution of routes from other routing protocols using IS-IS.	disable
metric <0-4261412864>	Redistribution metric.	10
metric-type {external   internal}	Select external or internal for the metric type.	external
level {level-1   level-1-2   level-2}	Set the IS-IS level to use for redistributing routes: <ul style="list-style-type: none"> <li>level-1: intra-area</li> <li>level-1-2: both intra-area and inter-area</li> <li>level-2-only: inter-area</li> </ul>	level1-2
routermap <string>	Enter the route map name. Only the route maps for this protocol are listed. You must create the route map before selecting it. See <a href="#">config router route-map on page 83</a> .	No default

Variable	Description	Default
<b>config redistribute6 {bgp6   connected   ospf6   ripng   static}</b>	Configure the IS-IS redistribute IPv6 protocols.	
status {disable   enable}	Enable or disable the redistribution of routes from other routing protocols using IS-IS.	disable
metric <0-4261412864>	Redistribution metric.	10
level {level-1   level-1-2   level-2}	Set the IS-IS level to use for redistributing routes: <ul style="list-style-type: none"> <li>level-1: intra-area</li> <li>level-1-2: both intra-area and inter-area</li> <li>level-2-only: inter-area</li> </ul>	level1-2
routemap <string>	Enter the route map name. Only the route maps for this protocol are listed. You must create the route map before selecting it. See <a href="#">config router route-map on page 83</a> .	No default
<b>config summary-address</b>	Configure the summarizing IPv4 address ranges in the IS-IS routing table.	
<summary address entry identifier>	Enter the summary address entry ID. The value range is 0-4294967295.	No default
level {level-1   level-1-2   level-2}	Set the IS-IS level to use for the summary database: <ul style="list-style-type: none"> <li>level-1: intra-area</li> <li>level-1-2: both intra-area and inter-area</li> <li>level-2-only: inter-area</li> </ul>	level-2
prefix <IPv4 address and netmask>	Set the IPv4 address and netmask for the prefix.	No default
<b>config summary-address6</b>	Configure the summarizing IPv6 address ranges in the IS-IS routing table.	
<summary address entry identifier>	Enter the summary address entry ID. The value range is 0-4294967295.	No default
level {level-1   level-1-2   level-2}	Set the IS-IS level to use for the summary database: <ul style="list-style-type: none"> <li>level-1: intra-area</li> <li>level-1-2: both intra-area and inter-area</li> <li>level-2-only: inter-area</li> </ul>	level-2
prefix6 <IPv6 address and netmask>	Set the IPv6 address and netmask for the prefix.	No default

## Example

The following is an example of an IS-IS configuration for IPv4 traffic:

```
config router isis
  set default-information-metric 60
  config interface
    edit "vlan100"
      set circuit-type level-1
      set priority-l1 80
      set wide-metric-l1 200
```

```

    next
    edit "vlan102"
        set circuit-type level-2
    next
end
config net
    edit 1
        set net 49.0002.0000.0000.1048.00
    next
end
set metric-style wide
config redistribute "connected"
    set status enable
end
config redistribute "rip"
end
config redistribute "ospf"
end
config redistribute "bgp"
end
config redistribute "static"
end
end
end

```

## config router key-chain

Use this command to configure a key chain. A key chain 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.

### Syntax

```

config router key-chain
    edit <key_chain_name>
        config key
            edit <key_chain_int>
                set key-string <key_str>
                set accept-lifetime <START> <END>
                set send-lifetime <START> <END>
            next
        end
    next
end

```

Variable	Description	Default
<key_chain_name>	Enter a name for your key chain.	No default
<b>config key</b>	Configure the key.	
<key_chain_int>	Enter the key chain identifier.	No default
key-string <key_str>	Enter a password string for the key.	No default

Variable	Description	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: <ul style="list-style-type: none"> <li>• HH:MM:SS is the time of day then the lifetime starts in hours, minutes, and seconds.</li> <li>• DAY is the day of the month to start. The range is 1-31.</li> <li>• MONTH is the month of the year to start. The range is 1-12.</li> <li>• YEAR is the year to start. The range is 1993-2035.</li> </ul> END can also be set to <i>infinite</i> 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: <ul style="list-style-type: none"> <li>• HH:MM:SS is the time of day then the lifetime starts in hours, minutes, and seconds.</li> <li>• DAY is the day of the month to start. The range is 1-31.</li> <li>• MONTH is the month of the year to start. The range is 1-12.</li> <li>• YEAR is the year to start. The range is 1993-2035.</li> </ul> END can also be set to <i>infinite</i> 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 key chain:

```
config router key-chain
  edit keychain1
    config key
      edit 1
        set accept-lifetime 12:00:00 09 01 2023 12:00:00 09 01 2024
        set key-string "keychain1"
        set send-lifetime 12:00:00 09 01 2025 12:00:00 09 01 2026
      next
    end
  next
end
```

## config router multicast

A FortiSwitch unit can operate as a Protocol Independent Multicast (PIM) version-4 router. FortiSwitchOS supports PIM source-specific multicast (SSM) and version 3 of Internet Group Management Protocol (IGMP).

You can configure a FortiSwitch unit to support PIM using the `config router multicast` CLI command. When PIM is enabled, the FortiSwitch unit allocates memory to manage mapping information. The FortiSwitch unit communicates with neighboring PIM routers to acquire mapping information and, if required, processes the multicast traffic associated with specific multicast groups.

## Syntax

```

config router multicast
  set multicast-routing {disable | enable}
  config interface
    edit {interface_name | internal | mgmt}
      set pim-mode ssm-mode
      set hello-interval <1-180 seconds>
      set dr-priority <1-4294967295>
      set multicast-flow <string>
    config igmp
      set query-interval <1-1800 seconds>
      set query-max-response-time <1-25 seconds>
    end
  end
end

```

Variable	Description	Default
multicast-routing {disable   enable}	Enable or disable multicast routing.	disable
{interface_name   internal   mgmt}	Set which interface to configure for multicast routing.	No default
pim-mode ssm-mode	Set the PIM operation mode to SSM mode.	ssm-mode
hello-interval <1-180 seconds>	Specify the amount of time that the FortiSwitch unit waits between sending hello messages to neighboring PIM routers.	30
dr-priority <1-4294967295>	Assign a priority to the FortiSwitch unit Designated Router (DR) candidacy. The value is compared to that of other DR interfaces connected to the same network segment, and the router having the highest DR priority is selected to be the DR. If two DR priority values are the same, the interface having the highest IP address is selected.	1
multicast-flow <string>	Connect the named multicast flow to this interface. You must create the multicast flow before it can be selected here. See <a href="#">config router multicast-flow on page 59</a> .	No default
<b>config igmp</b>	Configure the multicast-flow entries.	
query-interval <1-1800 seconds>	Set the interval between queries to IGMP hosts.	125
query-max-response-time <1-25 seconds>	Set the maximum time to wait for an IGMP query response.	10

## config router multicast-flow

Use this command to configure the source allowed for a multicast flow when using PIM-SM or PIM-SSM.

### Syntax

```

config router multicast-flow
  edit <name>

```

```

set comments <string>
config flows
  edit <multicast-flow_entry_identifier>
    set group-addr <224-239.xxx.xxx.xxx>
    set group-addr-end <224-239.xxx.xxx.xxx>
    set source-addr <IP_address>
  end
end

```

Variable	Description	Default
<name>	Name of the multicast flow.	No default
<string>	Enter an optional description of the multicast flow.	No default
<multicast-flow_entry_Identifier>	Enter the multicast-flow entry identifier.	No default
group-addr <224-239.xxx.xxx.xxx>	Enter the starting multicast group address (IPv4).	0.0.0.0
group-addr-end <224-239.xxx.xxx.xxx>	Optional. Enter the ending multicast group address (IPv4). The range must not overlap other defined ranges.	0.0.0.0
source-addr <IP_address>	Enter an IP address for the multicast source (IPv4).	0.0.0.0

## config router ospf

Use this command to configure OSPF routing for IPv4.

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

### Syntax

```

config router ospf
  set router-id <router_ipv4>
  set abr-type {cisco | ibm | shortcut | standard}
  set database-overflow {enable | disable}
  set database-overflow-max-external-lsa <integer>
  set database-overflow-time-to-recover <integer>
  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 distance <distance_int>
  set rfc1583-compatible {disable | enable}
  set spf-timers <delay_int> <hold_int>
  set log-neighbour-changes {disable | enable}
  set passive-interface <name_str>
config area
  edit <area_ipv4>
    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-status {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>
  next
end
next
end
config interface
  edit <interface_str>
    set authentication {md5 | none | text}
    set cost <cost_int>
    set dead-interval <dead_int>
    set hello-interval <hello_int>
    set mtu <mtu_int>
    set mtu-ignore {disable | enable}
    set priority <priority_int>
    set retransmit-interval <retransmit_int>
    set transmit-delay <transmit_int>
    set ttl <1-255>
    config md5-keys
      edit <key_ID>
        set key <MD5_key>
      next
    end
  next
end
next
end
config network
  edit <network_int>
    set area <area_ipv4>
    set prefix <xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx>
  end
end
config summary-address
  edit <summary_int>
    set prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
```

```
        set tag <tag_int>
    next
end
config distribute-list
    edit <distribute_int>
        set access-list <access_str>
        set protocol {bgp | connected | isis | rip | static}
    next
end
config redistribute {bgp | connected | isis | rip | static}
    set status {disable | enable}
    set metric <metric_int>
    set routemap <routemap_str>
    set metric-type {1 | 2}
    set tag <0-2147483647>
end
config vrf
    edit <VRF_ID>
        set abr-type {cisco | ibm | shortcut | standard}
        set database-overflow {enable | disable}
        set database-overflow-max-external-lsa <integer>
        set database-overflow-time-to-recover <integer>
        set default-information-metric <metric_int>
        set default-information-metric-type {1 | 2}
        set default-information-originate {always | disable | enable}
        set distance <distance_int>
        set distance-external <external_int>
        set distance-inter-area <inter_int>
        set distance-intra-area <intra_int>
        set log-neighbour-changes {disable | enable}
        set passive-interface <name_str>
        set rfc1583-compatible {disable | enable}
        set router-id <router_ipv4>
        set spf-timers <delay_int> <hold_int>
        config area
            edit <area_ipv4>
                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
            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-status {enable | disable}
            end
        end
        config virtual-link
            edit <virtual_int>
```

```
        set authentication {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>
    next
end
next
config interface
edit <interface_str>
    set authentication {none | text}
    set cost <cost_int>
    set dead-interval <dead_int>
    set hello-interval <hello_int>
    set mtu <mtu_int>
    set mtu-ignore {disable | enable}
    set priority <priority_int>
    set retransmit-interval <retransmit_int>
    set transmit-delay <transmit_int>
    config md5-keys
        edit <key_ID>
            set key <MD5_key>
        next
    end
next
end
config network
edit <network_int>
    set area <area_ipv4>
    set prefix <xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx>
end
end
config summary-address
edit <summary_int>
    set prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
    set tag <tag_int>
next
end
config distribute-list
edit <distribute_int>
    set access-list <access_str>
    set protocol {bgp | connected | isis | rip | static}
next
end
config redistribute {connected | rip | static}
    set status {disable | enable}
    set metric <metric_int>
    set routemap <routemap_str>
    set metric-type {1 | 2}
    set tag <0-2147483647>
next
end
next
end
```

Variable	Description	Default
router-id <router_ipv4>	Required. Enter the IPv4 address of the OSPF router.	No default
abr-type {cisco   ibm   shortcut   standard}	Enter the area border router (ABR) type. Set <code>abr-type</code> to <code>cisco</code> or <code>ibm</code> 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
database-overflow {enable   disable}	Enable or disable protection against link-state database overflow.	disable
database-overflow-max-external-lsa <integer>	Set the maximum number of external link-state advertisements (LSAs) that are allowed in the link-state database. The value range is 0-2147483647. This option is available only if <code>database-overflow</code> is enabled.	10000
database-overflow-time-to-recover <integer>	Set the number of seconds before the router originates any external LSAs. The value range is 0-65535 seconds. This option is available only if <code>database-overflow</code> is enabled.	300
distance-external <external_int>	Set the OSPF route administrative external distance. The value range is from 0 to 255.	No default
distance-inter-area <inter_int>	Set the OSPF route administrative inter-area distance. The value range is from 0 to 255.	No default
distance-intra-area <intra_int>	Set the OSPF route administrative intra-area distance. The value range is from 0 to 255.	No default
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 <code>default-information-metric</code> value and the metric type specified by the <code>default-information-metric-type</code> value. Set the value to <code>always</code> 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
distance <distance_int>	Set the OSPF route administrative distance. 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

Variable	Description	Default
log-neighbour-changes {disable   enable}	Enable or disable the logging of changes to the OSPF neighbor.	enable
passive-interface <name_str>	Select which interface to set to passive mode. <b>NOTE:</b> You need to add the interface prefix under the config network command (under config router ospf).	No default
<b>config area</b>	Configure the OSPF area.	
<area_ipv4>	Enter the IP address for the area.	No default
shortcut {default   disable   enable}	Enable or disable whether shortcuts are allowed in the area.	default
type {nssa   regular   stub}	Set the area type. <b>NOTE:</b> This field is not applicable for the backbone area (0.0.0.0), which is set to regular type by default.	regular
default-cost <cost_int>	If the area type is stub or not-so-stubby area (NSSA), set the cost of default-summary 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
<b>config filter-list</b>	Configure the OSPF area 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
<b>config range</b>	Configure the OSPF area 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-status {enable   disable}	Enable or disable whether the substitute prefix is used instead of the prefix.	disable
<b>config virtual-link</b>	Configure the OSPF virtual link.	

Variable	Description	Default
<virtual_int>	Enter the virtual-link identifier.	No 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>	Set the time between retransmitting lost link-state advertisement packets.	5
transmit-delay <transmit_int>	Enter the link-state packet transmit delay.	1
<b>config md5-keys</b>	These commands are applicable only when the virtual-link authentication field is set to md5.	
<key_ID>	Enter the MD5 key identifier.	No default
<MD5_key>	Enter a string up to 16 characters.	No default
<b>config interface</b>	Configure the 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}	Enable or disable BFD on this interface.	disable
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
mtu <mtu_int>	Enter the maximum transmission unit (MTU) size in bytes for the database description packets. The value range is 576-65535.	Not set
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>	Set the time between retransmitting lost link-state advertisement packets.	5
transmit-delay <transmit_int>	Enter the link-state transmit delay.	1
ttl <1-255>	Specify how many seconds unicast and multicast messages are kept.	0

Variable	Description	Default
<b>config md5-keys</b>	Use these commands to add MD5 keys for the OSPF interface. These commands are applicable only when the interface authentication field is set to md5.	
<key_ID>	Enter the MD5 key identifier.	No default
<MD5_key>	Enter a string up to 16 characters.	No default
<b>config network</b>	Use these commands to enable or disable OSPF on an IP network.	
<network_int>	Enter the network identifier.	No default
<area_ipv4>	Enter the IPv4 address for the area.	No default
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the IPv4 address and netmask.	No default
<b>config summary-address</b>	Configure the aggregate address for redistributed routes.	
<summary_int>	Enter the identifier for the summary address.	No default
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the IPv4 address and netmask.	No default
set tag <tag_int>	Enter the tag value. The range is 0-2147483647.	0
<b>config distribute-list</b>	Configure the redistribute routes filter.	
<distribute_int>	Enter the distribute list identifier.	No default
access-list <access_str>	Enter the access list name.	No default
protocol {bgp   connected   isis   rip   static}	Set the protocol type.	connected
<b>config redistribute {bgp   connected   isis   rip   static}</b>	Use these commands for the redistribute configuration.	
redistribute {bgp   connected   isis   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
route-map <route-map_str>	Enter the route map name to filter the redistributed routes. Only the route maps for this protocol are listed.	No default
metric-type {1   2}	Set the metric type of redistributed routes.	2
tag <0-2147483647>	Set the tag value.	No default
<b>config vrf</b>	Use these commands to create multiple routing tables within the same router.	
<VRF_ID>	Use the same VRF identifier that was configured under the <code>config router vrf</code> command. The commands under <code>config vrf</code> are the same as the commands under <code>config router ospf</code> .	No default

## Example

This example shows how to set the router identifier, create an area, configure the OSPF interface, create the network (set the network prefix and associate with an area), configure the IPv4 address summary, and redistribute the routes:

```
config router ospf

    set router-id 20.1.1.1

config area
    edit 0.0.0.0
    next
    edit 0.0.0.1
    next
end

config interface
    edit "ospf_1"
        set interface "vlan10"
    next
    edit "ospf_2"
        set interface "vlan20"
    next
end

config network
    edit 1
        set area 0.0.0.1
        set prefix 20.1.1.0 255.255.255.0
    next
    edit 2
        set area 0.0.0.0
        set prefix 10.1.1.0 255.255.255.0
    next
end

config summary-address
    edit 1
        set prefix 40.1.0.0 255.255.0.0
    next
end

config redistribute "connected"
    set status enable
end

end
```

## config router ospf6

Use this command to configure open shortest path first (OSPF) routing for IPv6.

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

## Syntax

```

config router ospf6
  set router-id <router_ipv4>
  set spf-timers <delay_int> <hold_int> <max_int>
  set log-neighbor-changes {disable | enable}
  config area
    edit <area_ipv4>
      set type {regular | stub}
      set stub-type {summary | no-summary}
      config filter-list
        edit <filter_int>
          set direction {in | out}
          set list <list_str>
        next
      end
    config range
      edit <range_int>
        set advertise {enable | disable}
        set prefix <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>
      next
    end
  next
end
config interface
  edit <interface_str>
    set area-id <Required_IPv4_address>
    set bfd {disable | enable}
    set cost <cost_int>
    set dead-interval <dead_int>
    set hello-interval <hello_int>
    set passive {disable | enable}
    set priority <priority_int>
    set retransmit-interval <retransmit_int>
    set status {enable | disable}
    set transmit-delay <transmit_int>
  next
end
config redistribute {connected | static}
  set status {disable | enable}
  set routemap <routemap_str>
end
end

```

Variable	Description	Default
router-id <router_ipv4>	Required. Enter the IPv4 address of the OSPF router.	No default

Variable	Description	Default
spf-timers <delay_int> <hold_int> <max_int>	Set the number of milliseconds to delay before the shortest path first (SPF) is calculated, the initial number of milliseconds between consecutive SPF calculations, and the maximum number of milliseconds between consecutive SPF calculations. The range for each value is from 0 to 600.	5 10 10
log-neighbor-changes {disable   enable}	Enable or disable the logging of changes to the OSPF neighbor	enable
<b>config area</b>	Configure the OSPF6 area.	
<area_ipv4>	Enter the IPv4 address for the area.	No default
type {regular   stub}	Set the area type to regular or stub.	regular
stub-type {summary   no-summary}	If the type is set to stub, set the stub type to summary or no summary.	summary
<b>config filter-list</b>	Configure the OSPF6 area 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 IPv6 access-list name or IPv6 prefix-list name for the area.	No default
<b>config range</b>	Configure the OSPF6 area 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 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>	Required. Enter the IPv6 prefix.	No default
<b>config interface</b>	Configure the OSPF6 interface.	
<interface_str>	Enter the OSPF interface name.	No default
area-id <IPv4_address>	Required. Enter the IPv4 address of the area.	none
bfd {disable   enable}	Enable or disable bidirectional forwarding detection (BFD).	disable
cost <cost_int>	Enter the link cost on this interface. The value range is 0-65535.	10
dead-interval <dead_int>	Enter the dead interval.	40

Variable	Description	Default
hello-interval <hello_int>	Enter the hello interval.	10
passive {disable   enable}	Enable or disable the passive interface.	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 time between retransmitting lost link-state advertisement packets.	5
status {enable   disable}	Enable or disable the IPv6 OSPF routing on this interface.	enable
transmit-delay <transmit_int>	Enter the link-state transmit delay.	1
<b>config redistribute {connected   static}</b>	Use these commands for the redistribute configuration.	
status {disable   enable}	Enable or disable the redistribution.	disable
routemap <routemap_str>	Enter the route map name to filter the redistributed routes. Only the route maps for this protocol are listed.	No default

## Example

This example shows how to set the router identifier, create an area, configure the OSPF interface, and redistribute the routes:

```

config router ospf6
  set router-id 10.11.101.1
  config area
    edit 0.0.0.1
      config filter-list
        edit 1
          set direction in
          set list access1
        next
      end
      config range
        edit 1
          set advertise disable
          set prefix 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234/96
        next
      end
    end
  end
  config interface
    edit vlan35
      set area 0.0.0.1

```

```

                set cost 100
                set priority 100
                set status enable
            next
        end
    config redistribute connected
        set status enable
    end
end

```

## config router policy

Use this command to create a policy to control routing.

### Syntax

```

config router policy
  config nexthop-group
    edit <name_of_next-hop_group>
      config nexthop
        edit <configuration_identifier>
          set nexthop-ip <IPv4_address>
          set nexthop-vrf-name <string>
        next
      end
    next
  end
  config pbr-map
    edit <PBR_map_name>
      set comments <string>
      config rule
        edit <rule_sequence_number>
          set src <IPv4_address_mask>
          set dst <IPv4_address_mask>
          set nexthop-ip <IPv4_address>
          set nexthop-vrf-name <string>
          set nexthop-group name <string>
        next
      end
    next
  end
  config interface
    edit <interface_name>
      set pbr-map-name <PBR_policy_map_name>
    next
  end
end

```

Variable	Description
<b>config nexthop-group</b>	Configure the next-hop group using equal-cost multi-path (ECMP) routing.

Variable	Description	
<name_of_next-hop_group>	Enter the name of the next-hop group.	No default
<b>config nexthop</b>	Configure the next hop.	
<configuration_identifier>	Enter the configuration identifier.	No default
nexthop-ip <IPv4_address>	Enter the IPv4 address of the next hop.	0.0.0.0
nexthop-vrf-name <string>	Enter the virtual routing and forwarding (VRF) instance name.	No default
<b>config pbr-map</b>	Configure the policy-based routing (PBR) map.	
<PBR_map_name>	Enter the name of the PBR map.	No default
comments <string>	Enter a descriptive comment.	No default
<b>config rule</b>	Configure the PBR rule.	
<rule_sequence_number>	Enter a rule identifier. The range of values is 1-10000.	No default
src <IPv4_address_mask>	Enter the source IPv4 address and mask.	0.0.0.0 0.0.0.0
dst <IPv4_address_mask>	Enter the destination IPv4 address and mask.	0.0.0.0 0.0.0.0
nexthop-ip <IPv4_address>	Enter the IPv4 address of the next hop.	0.0.0.0
nexthop-vrf-name <string>	Enter the name of the VRF instance that the next-hop address belongs to. If the name is not specified, the default VRF is used.	No default
nexthop-group name <string>	Enter the next-hop group name. This setting is used for ECMP.	No default
<b>config interface</b>	Configure the interface.	
<interface_name>	Enter the name of the interface to configure.	No default
pbr-map-name <PBR_map_name>	Enter the name of the PBR map. The PBR map is created with the config pbr-map command.	No default

## Example

This example creates the “pbrmap1” policy for vlan10, which is an ingress switch virtual interface (SVI). The policy has three rules:

- Rule 1 finds packets with a source address of 22.1.1.0/24 and forwards them to the next hop, 12.1.1.2, which belongs to the default VRF instance.
- Rule 2 finds packets with a destination address of 33.1.1.0/24 and forwards them to the ECMP route with the two next-hop IP addresses in the next-hop group . Both next hops belong to the default VRF instance.
- Rule 3 finds packets with a destination address of 11.1.1.0/24 and forwards them to the next hop, 13.1.1.2, which belongs to the “vrfv4” VRF instance.

```
config router policy
  config nexthop-group
    edit "nhgroup1"
      config nexthop
        edit 1
          set nexthop-ip 12.1.1.4
        next
      next
    next
  next
```

```
        edit 2
          set nexthop-ip 12.1.1.5
        next
      end
    next
  end
config pbr-map
  edit "pbrmap1"
    config rule
      edit 1
        set src 22.1.1.0 255.255.255.0
        set nexthop-ip 12.1.1.2
      next
      edit 2
        set dst 33.1.1.0 255.255.255.0
        set nexthop-group-name "nhgroup1"
      next
      edit 3
        set src 11.1.1.0 255.255.255.0
        set nexthop-ip 13.1.1.2
        set nexthop-vrf-name "vrfv4"
      next
    end
  next
end
config interface
  edit "vlan10"
    set pbr-map-name "pbrmap1"
  next
end
end
```

## config router prefix-list

Use this command to configure IPv4 prefix-based filtering.

### 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
end
```

Variable	Description	Default
<list_int>	Enter the prefix list identifier.	No default
comments <comment_str>	Enter a descriptive comment.	No default
<b>config rule</b>	Configure the prefix-list rule.	
<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
ge <ge_int>	Enter the minimum IPv4 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 IPv4 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 prefix-list6

Use this command to configure IPv6 prefix-based filtering.

### Syntax

```
config router prefix-list6
  edit <name_of_IPv6_prefix_list>
    set comments <string>
    config rule
      edit <rule_ID>
        set action {deny | permit}
        set prefix6 {<IPv6_prefix> | any}
        set ge <0-128>
        set le <0-128>
      next
    end
  end
```

Variable	Description	Default
<name_of_IPv6_prefix_list>	Enter the name of the IPv6 prefix list.	No default
comments <string>	Enter a descriptive comment.	No default
<b>config rule</b>	Configure the IPv6 prefix list rule.	
<rule_ID>	Enter the rule identifier.	No default
action {deny   permit}	Set the action to deny or permit.	permit
prefix6 {<IPv6_prefix>   any}	Enter the IPV6 prefix to match or any.	No default

Variable	Description	Default
ge <0-128>	Enter the minimum IPv6 prefix length to be matched. The IPv6 prefix list is used if the prefix length is greater than or equal to this value.	No default
le <0-128>	Enter the maximum IPv6 prefix length to be matched. The IPv6 prefix list is used if the prefix length is less than or equal to this value.	No default

## Example

This example shows how to specify which IPv6 prefixes are allowed in RA messages:

```
config router prefix-list6
  edit "r4"
    config rule
      edit 1
        set action deny
        set prefix6 "2001:4:4:4::4/64"
        set ge 65
        set le 128
      next
      edit 2
        set action permit
        set prefix6 "any"
      next
    end
  next
end
```

## config router rip

Use these commands to configure RIP routing with IPv4 addresses.

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

### 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>
  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 <key_chain_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 {bgp | connected | isis | ospf | static}
  set status {disable | enable}
  set metric <metric_int>
  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
default-metric <defaultmetric_int>	Enter the default metric for redistributed routes. This setting does not affect connected routes. The range of values is 1-16. 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. The range of values is 5-2147483647.	120

Variable	Description	Default
passive-interface <name_str>	Specify which interface to set to passive mode. You need to add the interface prefix under config network (under config router rip).	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. The range of values is 5-2147483647.	180
update-timer <update_int>	Enter the number of seconds between when the complete routing table is sent to neighboring RIP routers. The range of values is 5-2147483647.	30
version {1   2}	Set the RIP version for receiving and sending RIP packets.	2
<b>config distance</b>	Set the admin distance based on the route prefix and RIP neighbor IP.	
<distanceid_int>	Enter the distance identifier.	No default
access-list <access_string>	Enter the access list to match RIP routes.	No default
distance <distance_int>	Enter the RIP admin distance. The value range is from 1 to 255.	120
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the RIP neighbor IP prefix. Enter 0.0.0.0/0 to match all RIP neighbors.	0.0.0.0 0.0.0.0
<b>config distribute-list</b>	Filter networks from routing updates.	
<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
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
<b>config interface</b>	RIP interface configuration.	
<interface_str>	Enter the interface name.	No default
auth-keychain <key_chain_str>	Enter the name of the key chain 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.  <b>NOTE:</b> You must create a key chain first before you can use the MD5 authentication mode with RIP version 2.	none

Variable	Description	Default
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
<b>config neighbor</b>	Specify a neighbor router. These commands are required only when OSPF runs on nonbroadcast media.	
<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
<b>config network</b>	Enable RIP routing on an IP network.	
<network_int>	Enter a network identifier.	No default
prefix <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>	Enter the prefix.	No default
<b>config offset-list</b>	Configure the offset list to modify the RIP metric.	
<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.	enable
<b>config redistribute {bgp   connected   isis   ospf   static}</b>	Redistribute configuration.	
redistribute {bgp   connected   isis   ospf   static}	Redistribute routes so that they are included in RIP routing.	No default
status {disable   enable}	Enable or disable whether the routes are redistributed.	disable

Variable	Description	Default
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. Only the route maps for this protocol are listed.	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 ripng

Use these commands to configure RIP routing with IPv6 addresses.

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

### Syntax

```
config router ripng
  set bfd {disable | enable}
  set default-information-originate {disable | enable}
  set default-metric <defaultmetric_int>
  set garbage-timer <garbage_int>
  set timeout-timer <timeout_int>
  set update-timer <update_int>
  config aggregate-address
    edit <aggregate-address_entry_ID_int>
      set prefix6 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/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 passive {disable | enable}
    set split-horizon-status {disable | enable}
    set split-horizon {poisoned | regular}
  end
config offset-list
  edit <offsetlist_int>
    set access-list6 <accesslist_str>
    set direction {in | out}
    set interface {in | out}
    set offset <offset_int>
    set status {disable | enable}
  end
config redistribute {bgp | connected | isis | ospf6 | static}
  set status {disable | enable}
  set metric <metric_int>
  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
default-metric <defaultmetric_int>	Enter the default metric for redistributed routes. This setting does not affect connected routes. Use the <code>config redistribute connected</code> command to set the metric value for connected routes. The range of values is 1-16.	1
garbage-timer <garbage_int>	Enter the number of seconds before a route is removed from the routing table after it is no longer valid. The range of values is 5-2147483647.	120
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 garbage timer expires. The range of values is 5-2147483647.	180
update-timer <update_int>	Enter the number of seconds between when the complete routing table is sent to neighboring RIP routers. The range of values is 5-2147483647.	30
<b>config aggregate-address</b>	Set the aggregate RIPng route announcement.	
<aggregate-address_entry_ID_int>	Enter the identifier for the aggregate-address entry.	No default entry.

Variable	Description	Default
prefix6 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx>	Enter the IPv6 prefix.	No default
<b>config distribute-list</b>	Filter networks in routing updates.	
<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
listname <listname_str>	Enter the IPv6 access or prefix list name.	No default
status {disable   enable}	Enable or disable whether the distribute list is used.	enable
<b>config interface</b>	RIPng interface configuration.	
<interface_str>	Enter the interface name.	No default
passive {disable   enable}	Enable or disable whether to suppress routing updates on an interface.	disable
split-horizon-status {disable   enable}	Enable or disable split horizon.	enable
split-horizon {poisoned   regular}	Set the split-horizon type.	regular
<b>config offset-list</b>	Configure the offset list to modify the RIPng metric.	
<offsetlist_int>	Enter the offset list identifier.	No default
access-list6 <accesslist_str>	Enter the name of the IPv6 access list.	No default
direction {in   out}	Set the list direction.	out
interface {in   out}	Set the interface to which the offset-list will be applied.	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.	enable
<b>config redistribute {bgp   connected   isis   ospf6   static}</b>	Redistribute configuration.	
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. Only the route maps for this protocol are listed.	No default

## config router route-map

Use this command to configure a route map for BGP, IS-IS, OSPF, or RIP routing.

**NOTE:** You must have an advanced features license to use BGP, IS-IS, OSPF, or RIP routing.

### Syntax

```
config router route-map
edit <routemap_str>
set comments <comments_str>
set protocol {bgp | isis | isis6 | ospf | ospf6 | rip | ripng | zebra}
config rule
edit <rule_int>
set action {deny | permit}
set match-as-path <string>
set match-community <string>
set match-interface {<interface_str> | internal | mgmt}
set match-ip-address <address_str>
set match-ip6-address <access-list6 or prefix-list6>
set match-ip-nexthop <nexthop_str>
set match-metric <metric_int>
set match-origin {egp | igp | incomplete | none}
set match-tag <tag_int>
set set-aggregator-as <1-4294967295>
set set-aggregator-ip <IPv4_address>
set set-aspath <1-4294967295>
set set-atomic-aggregate {enable | disable}
set set-community-delete <string>
set set-community <community>
set set-extcommunity-rt <community>
set set-extcommunity-soo <community>
set set-ip-nexthop <class_ipv4>
set set-ip6-nexthop <IPv6_address>
set set-ip6-nexthop-local <IPv6_address>
set set-local-preference <1-4294967295>
set set-metric <setmetric_int>
set set-metric-type {1 | 2}
set set-origin {egp | igp | incomplete | none}
set set-originator-id <IP_address>
set set-tag <settag_int>
set set-weight <0-2147483647>
end
end
end
```

Variable	Description	Default
<routemap_str>	Enter the name for the individual route map.	No default
comments <comments_str>	Enter a descriptive comment.	No default

Variable	Description	Default
protocol {bgp   isis   isis6   ospf   ospf6   rip   ripng   zebra}	Mandatory. Set the protocol to BGP, IS-IS, OSPF (IPv4 or IPv6), RIP (IPv4 or IPv6), or the core router daemon.	No default
<b>config rule</b>	Configure the route-map rule.	
<rule_int>	Enter the rule identifier.	No default
action {deny   permit}	Set whether the rule permits or denies routes that match this rule.	permit
match-as-path <string>	Match the BGP Autonomous System (AS) path list.	No default
match-community <string>	Match the BGP community list.	No default
match-interface {<interface_str>   internal   mgmt}	Set which interface will be matched.	No default
match-ip-address <address_str>	Match the IPv4 address permitted by the IPv4 access list or IPv4 prefix list.	No default
match-ip6-address <access-list6 or prefix-list6>	Match the IPv6 address permitted by the IPv6 access list or IPv6 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>	Enter the metric to be matched for redistributed routes. The value range is 0-2147483647.	0
match-origin {egp   igp   incomplete   none}	Match the BGP origin code: <ul style="list-style-type: none"> <li>• egp—Set the value to the NLRI learned from the Exterior Gateway Protocol (EGP).</li> <li>• igp—Set the value to the NLRI learned from a protocol internal to the originating AS.</li> <li>• incomplete—Match routes that were learned some other way (for example, through redistribution).</li> <li>• none—Disable the matching of BGP routes based on the origin of the route.</li> </ul>	none
match-tag <tag_int>	Enter the tag to be matched. The value range is 0-2147483647.	0
set-aggregator-as <1-4294967295>	Set the BGP aggregator AS.	No default
set-aggregator-ip <IPv4_address>	Set the IPv4 address for the BGP aggregator.	0.0.0.0

Variable	Description	Default
	This option is visible only when set-aggregator-as is set.	
set-aspath <1-4294967295>	Prepend the BGP AS path attribute. Use quotation marks for repeating numbers, for example: "1 1 2"	No default
set-atomic-aggregate {enable   disable}	Enable or disable the BGP atomic aggregate attribute.	disable
set-community-delete <string>	Delete communities matching the community list.	No default
set-community <community>	Set the BGP community attribute: <ul style="list-style-type: none"> <li>Use decimal notation to set a specific COMMUNITY attribute for the route. The value has the syntax AA:NN, where AA represents an AS, and NN is the community identifier. Delimit complex expressions with double-quotation marks (for example, "123:234 345:456").</li> <li>To make the route part of the Internet community, select internet.</li> <li>To make the route part of the LOCAL_AS community, select local-AS.</li> <li>To make the route part of the NO_ADVERTISE community, select no-advertise.</li> <li>To make the route part of the NO_EXPORT community, select no-export.</li> </ul>	No default
set-extcommunity-rt <community>	Set the Route-Target extended community: AA:NN	No default
set-extcommunity-soo <community>	Set the Site-of-Origin extended community: AA:NN	No default
set-ip-nexthop <class_ipv4>	Enter the IPv4 address of the next hop.	0.0.0.0
set-ip6-nexthop <IPv6_address>	Enter the IPv6 global address of the next hop.	No default
set-ip6-nexthop-local <IPv6_address>	Enter the IPv6 local address of the next hop.	No default
set-local-preference <1-4294967295>	Set the BGP local-preference path attribute.	0
set-metric <setmetric_int>	Enter the route metric value. The value range is 0-2147483647.	0
set-metric-type {1   2}	Set the metric type to external-type1 or external-type2.	external-type1
set-origin {egp   igp   incomplete   none}	Set the BGP origin code: <ul style="list-style-type: none"> <li>egp—Set the value to the NLRI learned</li> </ul>	none

Variable	Description	Default
	<p>from the Exterior Gateway Protocol (EGP).</p> <ul style="list-style-type: none"> <li>• <code>igp</code>—Set the value to the NLRI learned from a protocol internal to the originating AS.</li> <li>• <code>incomplete</code>—If not <code>egp</code> or <code>igp</code>.</li> <li>• <code>none</code>—Disable the ORIGIN attribute.</li> </ul>	
<code>set-originator-id &lt;IP_address&gt;</code>	Set the BGP originator ID attribute.	0.0.0.0
<code>set-tag &lt;settag_int&gt;</code>	Enter the route tag value. The value range is 0-2147483647.	0
<code>set-weight &lt;0-2147483647&gt;</code>	Set the BGP weight for the routing table.	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
  end
```

## config router setting

Use this command to filter incoming protocol routes in RIB. You can filter protocol routes so that they are not added in the RIB routing table.

**NOTE:** You must have an advanced features license to use BGP, IS-IS, OSPF, or RIP routing.

### Syntax

```
config router setting
  config filter-list
    edit <filter_list_ID>
      set protocol {any | any6 | bgp | bgp6 | isis | isis6 | ospf | ospf6 | rip | ripng | static
        | static6}
      set route-map <route_map_name>
    end
```

```
end
```

Variable	Description	Default
<filter_list_ID>	Enter a filter-list identifier.	No default
protocol {any   any6   bgp   bgp6   isis   isis6   ospf   ospf6   rip   ripng   static   static6}	Specify which protocol routes that the filter will be applied to: <ul style="list-style-type: none"> <li>any: any IPv4 protocol.</li> <li>any6: any IPv6 protocol.</li> <li>bgp: IPv4 BGP.</li> <li>bgp6: IPv6 BGP.</li> <li>isis: IPv4 IS-IS.</li> <li>isis6: IPv6 IS-IS.</li> <li>ospf: IPv4 OSPF.</li> <li>ospf6: IPv6 OSPF.</li> <li>rip: IPv4 RIP.</li> <li>ripng: IPv6 RIP.</li> <li>static: IPv4 static.</li> <li>static6: IPv6 static.</li> </ul>	No default
route-map <route_map_name>	Enter the route map name. Only a route map created with the protocol set to zebra can be applied here.	No default

## Example

This example shows how to filter incoming protocol routes in RIB:

```
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 unit. 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.

### Syntax

```
config router static
  edit <sequence_number>
    set bfd {enable | disable}
    set blackhole {enable | disable}
    set comment <comment_str>
    set device <interface_name>
    set distance <1-255>
```

```

set dst <destination-address_IPv4mask>
set dynamic-gateway {enable | disable}
set gateway <gateway-address_IPv4>
set gw-l2-switch {enable | disable}
set status {enable | disable}
set vrf <string>
end

```

Variable	Description	Default
<sequence_number>	Enter a sequence number for the static route.	No default
bfd {enable   disable}	Enable or disable Bidirectional Forwarding for the route gateway.	disable
blackhole {enable   disable}	Enable or disable dropping all packets that match this route.	disable
comment <comment_str>	Optionally enter a descriptive comment.	No default
device <interface_name>	Enter the name of the interface through which to route traffic. Enter '?' to see a list of interfaces.	No default
distance <1-255>	Enter the administrative distance for the route. 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 0.0.0.0
dynamic-gateway {enable   disable}	When enabled, the route gateway IP is obtained using DHCP running on the provided route's device interface.	disable
gateway <gateway-address_IPv4>	Enter the IPv4 address of the next-hop router to which traffic is forwarded.	No default
gw-l2-switch {enable   disable}	Enable or disable the layer-2 gateway.	disable
status {enable   disable}	Enable this setting for the route to be added to the routing table.	enable
vrf <string>	Assign the specified virtual routing and forwarding (VRF) instance to this static route. After the static route is created, the VRF instance cannot be changed or unset.	No default

## Example

This example shows how to configure a static route:

```

config router static
  edit 1
    set gateway 192.168.0.10
    set status enable
  end
end

```

## config router static6

Use this command to add, edit, or delete static routes for IPv6 traffic.

You add static routes to manually control traffic exiting the FortiSwitch unit. 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.

### Syntax

```
config router static6
  edit <sequence_number>
    set bfd {enable | disable}
    set blackhole {enable | disable}
    set comment <comment_str>
    set device <interface_name>
    set distance <1-255>
    set dst <destination-address_IPv6mask>
    set gateway <gateway-address_IPv6>
    set status {enable | disable}
    set vrf <string>
  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.	No default
bfd {enable   disable}	Enable or disable bidirectional forwarding detection (BFD) for the gateway.	disable
blackhole {enable   disable}	Enable or disable dropping all packets that match this route.	disable
comment <comment_str>	Optionally enter a descriptive comment.	No default
device <interface_name>	Enter the name of the interface through which to route traffic. Enter '?' to see a list of interfaces.	No default
distance <1-255>	Enter the administrative distance for the route. The range is an integer from 1-255.	10
dst <destination-address_IPv6mask>	Enter the destination IPv6 address and network mask for this route.	::/0
gateway <gateway-address_IPv6>	Enter the IPv6 address of the next-hop router to which traffic is forwarded.	::
status {enable   disable}	Enable this setting for the route to be added to the routing table.	enable

Variable	Description	Default
vrf <string>	Assign the specified virtual routing and forwarding (VRF) instance to this static route.  After the static route is created, the VRF instance cannot be changed or unset.	No default

## Example

This example shows how to configure a static route for IPv6 traffic:

```
config router static6
  edit 1
    set dst 5555::/64
    set gateway 4000::2
    set status enable
  end
end
```

## config router vrf

Use these commands to create virtual routing and forwarding (VRF) instances.

### Syntax

```
config router vrf
  edit <VRF_name>
    set vrfid <integer>
  end
```

Variable	Description	Default
<VRF_name>	Enter the name of the VRF instance.  The name cannot match the name of any switch virtual interface (SVI).	No default
vrfid <integer>	Set the VRF identifier. The range of values is 1-1023.  You cannot use 252, 253, 254, or 255. After the VRF instance is created, the VRF ID cannot be changed.	0

## Example

This example shows how to configure two VRF instances:

```
config router vrf
  edit vrfv4
    set vrfid 1
  next
  edit vrfv6
    set vrfid 2
  next
end
```

# config switch

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

- [config switch acl 802-1X on page 92](#)
- [config switch acl egress on page 94](#)
- [config switch acl ingress on page 95](#)
- [config switch acl policer on page 99](#)
- [config switch acl prelookup on page 100](#)
- [config switch acl service custom on page 101](#)
- [config switch acl settings on page 103](#)
- [config switch auto-isl-port-group on page 103](#)
- [config switch auto-network on page 104](#)
- [config switch global on page 105](#)
- [config switch hsr ring on page 113](#)
- [config switch hsr settings on page 114](#)
- [config switch igmp-snooping globals on page 115](#)
- [config switch interface on page 116](#)
- [config switch ip-mac-binding on page 127](#)
- [config switch ip-source-guard on page 128](#)
- [config switch lldp profile on page 129](#)
- [config switch lldp settings on page 134](#)
- [config switch macsec profile on page 135](#)
- [config switch mirror on page 138](#)
- [config switch mld-snooping globals on page 142](#)
- [config switch mrp profile on page 142](#)
- [config switch mrp settings on page 143](#)
- [config switch network-monitor directed on page 144](#)
- [config switch network-monitor settings on page 145](#)
- [config switch phy-mode on page 146](#)
- [config switch physical-port on page 148](#)
- [config switch prp channel on page 153](#)
- [config switch prp settings on page 154](#)
- [config switch ptp settings on page 155](#)
- [config switch qos dot1p-map on page 156](#)
- [config switch qos ip-dscp-map on page 157](#)
- [config switch qos qos-policy on page 158](#)
- [config switch quarantine on page 161](#)
- [config switch rguard-policy on page 161](#)
- [config switch security-feature on page 163](#)
- [config switch static-mac on page 166](#)
- [config switch storm-control on page 167](#)
- [config switch stp instance on page 167](#)
- [config switch stp settings on page 169](#)

- [config switch trunk on page 170](#)
- [config switch virtual-port on page 173](#)
- [config switch virtual-wire on page 174](#)
- [config switch vlan on page 174](#)
- [config switch vlan-tpid on page 182](#)

## config switch acl 802-1X

Use this command to configure an 802.1x RADIUS dynamic ingress policy.

### Syntax

```
config switch acl 802-1X
  edit <policy_ID>
    set description <string>
    set filter-id <string>
    config access-list-entry
      edit <ingress_policy_ID>
        set description <string>
        set group <integer>
        config action
          set count {enable | disable}
          set drop {enable | disable}
        end
      config classifier
        set dst-ip-prefix <IP_address_and_netmask>
        set dst-mac <MAC_address>
        set ether-type <integer>
        set service <service_name>
        set src-ip-prefix <IP_address_and_netmask>
        set src-mac <MAC_address>
      end
    end
  next
end
next
end
next
end
```

Variable	Description	Default
<policy-id>	Enter the unique ID number of this policy.	No default
description <string>	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
filter-id <string>	Enter the filter-id of the policy. <b>NOTE:</b> Changing the name of filter-id after authentication causes errors in the output of the diagnose switch 802-1x status-dacl command when the session is using filter-id.	No default

Variable	Description	Default
<b>config access-list-entry</b>		
<ingress_policy_ID>	Enter the ingress policy identifier.	No default
description <string>	Enter a description of the policy.	No default
group <integer>	Enter the group ID of the policy. You can only enter 1.	1
<b>config action</b>		
count {enable   disable}	Enable or disable the count action.	disable
drop {enable   disable}	Enable or disable the drop action.	disable
<b>config classifier</b>		
dst-ip-prefix <IP_address_and_netmask>	Enter the destination IP address and subnet mask to be matched.	0.0.0.0 0.0.0.0
dst-mac <MAC_address>	Enter the destination MAC address to be matched.	00:00:00:00:00:00
ether-type <integer>	Enter the Ethernet type to be matched.	0x0000
service <service_name>	Enter the service name to be matched.	No default
src-ip-prefix <IP_address_and_netmask>	Enter the source IP address and subnet mask to be matched.	0.0.0.0 0.0.0.0
src-mac <MAC_address>	Enter the source MAC address to be matched.	00:00:00:00:00:00

## Example

This example shows how to configure an 802.1x RADIUS dynamic ingress policy.

```

config switch acl 802-1X
  edit 1
    set description "Test Filter-Id"
    set filter-id "Testing"
    config access-list-entry
      edit 1
        set description "Test ACL entry"
        config action
          set count enable
          set drop enable
        end
        config classifier
          set dst-ip-prefix 192.168.0.0 255.255.255.0
          set ether-type 0x0800
          set service "filter-id-service1"
          set src-ip-prefix 192.168.0.0 255.255.255.0
          set src-mac 00:00:00:00:00:00
        end
      end
    next
  end
next
end

```

## config switch acl egress

Use this command to configure an access control list (ACL) for an egress policy.

### Syntax

```
config switch acl egress
edit <policy_ID>
  set description <string>
  set interface <port_name>
  set schedule <schedule_name>
  set status {active | inactive}
  config classifier
    set cos <802.1Q CoS value to match>
    set dscp <DSCP value to match>
    set dst-ip-prefix <IP_address> <mask>
    set dst-mac <MAC_address>
    set ether-type <integer>
    set service <service_ID>
    set src-ip-prefix <IP_address> <mask>
    set src-mac <MAC_address>
    set vlan-id <VLAN_ID>
  end
  config action
    set count {enable | disable}
    set count-type {all | green | yellow}
    set drop {enable | disable}
    set mirror <mirror_session>
    set outer-vlan-tag <integer>
    set policer <policer>
    set redirect <interface_name>
    set remark-dscp <0-63>
  end
end
```

Variable	Description	Default
<policy-id>	Enter the unique ID number of this policy.	No default
description <string>	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
interface <port_name>	Interface that the policy applies to.	No default
schedule <schedule_name>	Select a schedule for when the ACL policy will be enforced.  The schedule must have been defined already with the <code>config system schedule</code> command.	No default
status {active   inactive}	Make the egress ACL policy active or inactive.	active
<b>config classifier</b>		

Variable	Description	Default
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
dst-ip-prefix <IP_address> <mask>	Destination IP address and subnet mask to be matched.	0.0.0.0 0.0.0.0
dst-mac <MAC_address>	Destination MAC address to be matched.	00:00:00:00:00:00
ether-type <integer>	Ethernet type to be matched.	0x0000
service <service_ID>	Service type to be matched.	No default
src-ip-prefix <IP_address> <mask>	Source IP address and subnet mask to be matched.	0.0.0.0 0.0.0.0
src-mac <MAC_address>	Source MAC address to be matched.	00:00:00:00:00:00
vlan-id <VLAN_ID>	VLAN identifier to be matched.	0
<b>config action</b>		
count {enable   disable}	Enable or disable the <b>count</b> action.	disable
count-type {all   green   yellow}	You can select <b>all</b> to count all egress packets, <b>green</b> to count egress packets if the traffic rate is within the guaranteed information rate, and <b>yellow</b> to count all other egress packets.	No default
drop {enable   disable}	Enable or disable the <b>drop</b> action.	disable
mirror <mirror_session>	Mirror session name.	No default
outer-vlan-tag <integer>	Outer VLAN tag.	0
policer <policer>	Identifier of the policer to associate with this policy. To create a policer, see <a href="#">config switch acl policer on page 99</a> .	0
redirect <interface_name>	Redirect interface name.	No default
remark-dscp <0-63>	Set the DSCP marking value.	No default

## config switch acl ingress

Use this command to configure an ACL for an ingress policy. Starting in FortiSwitchOS 6.2.0, you can create groups for multiple ingress ACLs. Starting in FortiSwitchOS 7.2.3, IPv6 addresses are supported.

### Syntax

```
config switch acl ingress
edit <policy-id>
  set description <string>
  set group <group_ID>
  set ingress-interface <port > [<port > ... <port >]
```

```

set ingress-interface-all {enable | disable}
set schedule <schedule_name>
set status {active | inactive}
config classifier
  set cos <802.1Q CoS value to match>
  set dscp <DSCP value to match>
  set dst-ip-prefix <IPv4_address> <mask>
  set dst-ip6-prefix <IPv6_address> <prefix>
  set dst-mac <MAC_address>
  set ether-type <integer>
  set service <service-id>
  set src-ip-prefix <IPv4_address> <mask>
  set src-ip6-prefix <IPv6_address> <prefix>
  set src-mac <MAC_address>
  set vlan-id <vlan-id>
end
config action
  set cos-queue <0-7>
  set count {enable | disable}
  set count-type {all | green | yellow | red}
  set cpu-cos-queue <integer>
  set drop {enable | disable}
  set egress-mask {<physical_port_name> | internal}
  set mirror <mirror_session>
  set outer-vlan-tag <integer>
  set policer <policer>
  set redirect <interface_name>
  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 <string>	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
group <group_ID>	Enter the group identifier of the policy. The range of group identifiers varies among the different platforms. Starting in FortiSwitchOS 6.2.0, you can create groups for multiple ingress ACLs. <b>NOTE:</b> The group identifier must be 3 or higher to be able to use IPv6 addresses.	1
ingress-interface <port > [<port > ... <port >]	If ingress-interface-all is disabled, enter the interface list to which the policy is bound on the ingress.	No default
ingress-interface-all {enable   disable}	If enabled, policy is bound to all interfaces.	disable

Variable	Description	Default
schedule <schedule_name>	Select a schedule for when the ACL policy will be enforced. The schedule must have been defined already with the <code>config system schedule</code> command.	No default
status {active   inactive}	Make the ingress ACL policy active or inactive.	active
<b>config classifier</b>		
cos <802.1Q CoS value to match>	Enter the 802.1Q CoS value to match. The range of values is 0-7.	0
dscp <DSCP value to match>	Enter the DSCP value to match. The range of values is 0-63.	0
dst-ip-prefix <IPv4_address> <mask>	Enter the destination IPv4 address and subnet mask to be matched.	0.0.0.0 0.0.0.0
dst-ip6-prefix <IPv6_address> <prefix>	Enter the destination IPv6 address and prefix to be matched. <b>NOTE:</b> You must set group to 3 or higher for this option to be available. If you are going to use a dynamic ACL, set group to 4 or higher.	::/0
dst-mac <MAC_address>	Enter the destination MAC address to be matched.	00:00:00:00:00:00
ether-type <integer>	Enter the Ethernet type to be matched. The range of values is 0-65535.	0x0000
service <service-id>	Enter the service type to be matched.	No default
src-ip-prefix <IPv4_address> <mask>	Enter the source IPv4 address and subnet mask to be matched.	0.0.0.0 0.0.0.0
src-ip6-prefix <IPv6_address> <prefix>	Enter the source IPv6 address and prefix to be matched. <b>NOTE:</b> You must set group to 3 or higher for this option to be available. If you are going to use a dynamic ACL, set group to 4 or higher.	::/0
src-mac <MAC_address>	Enter the source MAC address to be matched.	00:00:00:00:00:00
vlan-id <vlan-id>	Enter the VLAN identifier to be matched. The range of values is 1-4094.	0
<b>config action</b>		
cos-queue <0-7>	CoS queue number (0-7).	No default
count	Enable or disable the <b>count</b> action.	disable

Variable	Description	Default
count-type {all   green   yellow   red}	You can select all to count all ingress packets, green to count ingress packets if the traffic rate is within the guaranteed information rate, yellow to count ingress packets if they exceed the committed burst size but do not exceed the excess burst size, and red to count all other ingress packets.	No default
cpu-cos-queue <integer>	CPU CoS queue number. This CoS queue is only used if the packets reach the CPU. Enter <code>set cpu-cos-queue ?</code> to see the value range.	disabled
drop	Enable or disable the <b>drop</b> action.	disable
egress-mask {<physical_port_name>   internal}	List of physical ports to be configured in egress mask.	none
mirror <mirror_session>	Mirror session name.	No default
outer-vlan-tag	Outer VLAN tag. The range of values is 1-4094.	0
policer	Identifier of the policer to associate with this policy. To create a policer, see <a href="#">config switch acl policer on page 99</a> .	0
redirect <interface_name>	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
redirect-physical-port	List of ports to redirect the packet.	none
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 ingress
  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
    set status inactive
  next
  edit 2
    config classifier
      set vlan-id 3
```

```

    end
    set ingress-interface-all enable
    set status active
  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 ingress
  edit 1
    config classifier
      set src-mac 11:22:33:aa:bb:cc
      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
  set status active
end

```

## config switch acl policer

Use this command to configure an ACL policer for egress or ingress policies.

### 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>
    set type {egress | ingress}
  end

```

Variable	Description	Default
<policer index>	Enter the index for this ACL policer	No default
description <string>	Enter a text description for the policer.	No default
guaranteed-bandwidth <bandwidth_value>	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 <in_bytes>	Guaranteed burst size in bytes (max value = 4294967295)	0
maximum-burst <in_bytes>	Maximum burst size in bytes (max value = 4294967295)	0
type {egress   ingress}	Specify whether the policer is for egress or ingress policies.	ingress

## Example

This example shows how to configure an ACL policer for egress policies.

```
config switch acl policer
  edit 1
    set description policer1
    set guaranteed-bandwidth 8776000
    set guaranteed-burst 858993459
    set maximum-burst 4294967295
    set type egress
  end
```

## config switch acl prelookup

Use this command to configure an ACL for a lookup policy.

### Syntax

```
config switch acl prelookup
  edit <policy_ID>
    set description <string>
    set interface <port_name>
    set interface-all {enable | disable}
    set schedule <schedule_name>
    set status {active | inactive}
    config classifier
      set cos <802.1Q CoS value to match>
      set dscp <DSCP value to match>
      set dst-ip-prefix <IP_address> <mask>
      set dst-mac <MAC_address>
      set ether-type <integer>
      set service <service_ID>
      set src-ip-prefix <IP_address> <mask>
      set src-mac <MAC_address>
      set vlan-id <VLAN_ID>
    end
    config action
      set count {enable | disable}
      set cos-queue <0-7>
      set drop {enable | disable}
      set outer-vlan-tag <integer>
      set remark-cos <0-7>
    end
  end
```

Variable	Description	Default
<policy-id>	Enter the unique ID number of this policy.	No default

Variable	Description	Default
description <string>	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
interface <port_name>	Select which ingress interface that the policy applies to.	No default
interface-all {enable   disable}	Enable or disable whether the policy applies to all ingress interfaces.	disable
schedule <schedule_name>	Select a schedule for when the ACL policy will be enforced. The schedule must have been defined already with the <code>config system schedule</code> command.	No default
status {active   inactive}	Make the prelookup ACL policy active or inactive.	active
<b>config classifier</b>		
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
dst-ip-prefix <IP_address> <mask>	Destination IP address and subnet mask to be matched.	0.0.0.0 0.0.0.0
dst-mac <MAC_address>	Destination MAC address to be matched.	00:00:00:00:00:00
ether-type <integer>	Ethernet type to be matched.	0x0000
service <service_ID>	Service type to be matched.	No default
src-ip-prefix <IP_address> <mask>	Source IP address and subnet mask to be matched.	0.0.0.0 0.0.0.0
src-mac <MAC_address>	Source MAC address to be matched.	00:00:00:00:00:00
vlan-id <VLAN_ID>	VLAN identifier to be matched.	0
<b>config action</b>		
count {enable   disable}	Enable or disable the <i>count</i> action.	disable
cos-queue <0-7>	CPU CoS queue number (20-29). Only if packets reach to CPU. The value range is 20-29.	No default
drop {enable   disable}	Enable or disable the <i>drop</i> action.	disable
outer-vlan-tag <integer>	Outer VLAN tag.	0
remark-cos <0-7>	Set the CoS marking value. The range is 0-7.	No default

## 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 icmptype <0-255>
    set icmpcode <0-255>
    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 <string>	Add comments for the custom service.	No default
color <0-32>	Set the icon color to use in the Web-based manager. A value of zero sets the default color (1).	0
protocol {ICMP   IP   TCP/UDP/SCTP}	Select the protocol used by the service. These protocols are available when explicit-proxy is enabled.	TCP/UDP/SCTP
icmptype <0-255>	If you set the protocol to ICMP, set the ICMP type.	0
icmpcode <0-255>	If you set the protocol to ICMP, set the ICMP code.	0
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 ingress # 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 auto-isl-port-group

Use this command to create a multi-tiered MLAG trunk when the FortiSwitch unit is managed by a FortiGate unit.

## Syntax

```
config switch auto-isl-port-group
  edit <trunk_name>
    set members <one or more ports>
  end
```

## Example

The following example creates two trunks for a multi-tiered MCLAG:

```
config switch auto-isl-port-group
  edit "mclag-core1"
    set members "port1" "port2"
  next
  edit "mclag-core2"
    set members "port3" "port4"
  end
```

# config switch auto-network

Use this command to automatically form an inter-switch link (ISL) between two switches.



Starting in FortiSwitchOS 7.2.0, auto-network is enabled by default.

After an execute `factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it.

## Syntax

```
config switch auto-network
  set mgmt-vlan <1-4094>
  set status {enable | disable}
end
```

Variable	Description	Default
mgmt-vlan <1-4094>	Set the VLAN to use for the native VLAN on ISL ports and the native VLAN on the internal switch interface.	4094
status {enable   disable}	Enable or disable whether an ISL is automatically formed between two switches.	enable

## Example

The following example enables the automatic formation of an ISL between two switches:

```
config switch auto-network
  set mgmt-vlan 200
  set status enable
end
```

## config switch global

Use this command to configure system-wide FortiSwitch settings.

### Syntax

```
config switch global
  set allow-mac-move {enable | disable}
  set auto-fortilink-discovery {enable | disable}
  set auto-isl {enable | disable}
  set auto-isl-port-group <0-9>
  set auto-stp-priority {enable | disable}
  set bpdu-learn {enable | disable}
  set dhcp-snooping-database-export {disable | enable}
  set dmi-global-all {enable | disable}
  set flapguard-retain-trigger {enable | disable}
  set flood-unknown-multicast {enable | disable}
  set fortilink-heartbeat-timeout <0-300>
  set fortilink-p2p-native-vlan <integer>
  set fortilink-p2p-tpid <integer>
  set fortilink-vlan-optimization {enable | disable}
  set forti-trunk-dmac <xx:xx:xx:xx:xx:xx>
  set ip-mac-binding {enable | disable}
  set l2-memory-check {enable | disable}
  set l2-memory-check-interval <number_of_seconds>
  set log-mac-limit-violations {enable | disable}
  set log-source-guard-violations {enable | disable}
  set loop-guard-tx-interval <0-30>
  set mac-aging-interval <seconds>
  set mac-violation-timer <integer>
  set max-frame-size <bytes_int>
  set max-path-in-ecmp-group <integer>
  set mclag-igmpsnooping-aware {enable | disable}
  set mclag-peer-info-timeout <integer>
  set mclag-port-base <integer>
  set mclag-split-brain-all-ports-down {enable | disable}
  set mclag-split-brain-detect {enable | disable}
  set mclag-split-brain-priority <0-100>
  set mclag-stp-aware {enable | disable}
  set mirror-qos <0-7>
  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-guard-band <integer>
  set poe-power-budget <integer>
  set poe-power-mode {first-come-first-served | priority}
  set poe-pre-standard-detect {disable | enable}
  set qos-drop-policy {random-early-detection | taildrop}
  set qos-red-probability <integer>
  set reserved-mcast-to-cpu {enable | disable}
  set source-guard-violation-timer <integer>
  set storm-control-monitor {enable | disable}
  set storm-control-high-rate <0-65536>
```

```

set storm-control-rate-filter <0-100>
set trunk-hash-mode {default| enhanced}
set trunk-hash-unicast-src-port {enable | disable}
set trunk-hash-unkunicast-src-dst {enable | disable}
set virtual-wire-tpid <0x0001-0xfffe>
set vxlan-dport <integer>
set vxlan-sport <integer>
set vxlan-stp-virtual-mac <MAC_address>
set vxlan-stp-virtual-root {enable | disable}
set vxlan-qos-inner-to-outer {copy-to-outer | fixed}
set vxlan-qos-dscp <0-63>
config port-security
  set link-down-auth {no-action | set-unauth}
  set mab-entry-as {dynamic | static}
  set mab-reauth {enable | disable}
  set mac-called-station-delimiter {colon | hyphen | none | single-hyphen}
  set mac-calling-station-delimiter {colon | hyphen | none | single-hyphen}
  set mac-case {lowercase | uppercase}
  set mac-password-delimiter {colon | hyphen | none | single-hyphen}
  set mac-username-delimiter {colon | hyphen | none | single-hyphen}
  set max-reauth-attempt <0-15>
  set quarantine-vlan {enable | disable}
  set reauth-period <1-1440>
  set tx-period <12-60>
end
end

```

Variable	Description	Default
allow-mac-move {enable   disable}	Enable or disable the capability for the 802.1X client to move between ports that are not directly connected to the FortiSwitch unit without having to delete the 802.1X session.  This command is available only for the FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, and FS-148F-FPOE models.	disable
auto-fortilink-discovery {enable   disable}	Enable or disable the capability for the FortiGate device to automatically discover the FortiLink interface on the FortiSwitch unit.	enable
auto-isl {enable   disable}	Enable or disable the capability to automatically form an inter-switch LAG.	enable
auto-isl-port-group <0-9>	Set the ISL port group. The range is 0-9.	0
auto-stp-priority {enable   disable}	Enable or disable the automatic assigned STP switch priority.	enable
bpdu-learn {enable   disable}	Enable or disable bridge protocol data unit (BPDU) learning.	enable

Variable	Description	Default
	<b>NOTE:</b> This command is available on the following FortiSwitch models: FSR-124D, FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE, FS-424D, FS-424D-POE, FS-424D-FPOE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-POE, FS-448D-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE, FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE, FS-1024D, FS-1048D, FS-1048E, FS-3032D, and FS-3032E.	
dhcp-snooping-database-export {disable   enable}	Enable or disable whether the DHCP snooping database is exported to file.	disable
dmi-global-all {enable   disable}	Enable or disable DMI globally.	enable
flapguard-retain-trigger {enable   disable}	Enable this setting to keep the “triggered” status in the output of the diagnose flapguard status command after a switch has been rebooted until the port has been reset with the execute flapguard reset <port_name> command.  Disable this setting to reset the “triggered” status when the switch is rebooted.	disable
flood-unknown-multicast {enable   disable}	Enable or disable whether to flood the VLAN with unknown multicast messages.	disable
fortilink-heartbeat-timeout <0-300>	Set how long before the FortiLink heartbeat times out. Set the value to 0 to disable the FortiLink heartbeat.	60
fortilink-p2p-native-vlan <integer>	Specify the native VLAN on the inter-switch link (ISL) when fortilink-p2p is enabled under the config switch physical port command.	4094
fortilink-p2p-tpid <interger>	Set the FortiLink point-to-point TPID value. The range of values is 0x0001 to 0xfffe.  This command is only available in FortiLink mode.	0x8100
fortilink-vlan-optimization {enable   disable}	Enable or disable FortiLink VLAN optimization.	disable
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   disable}	Enable or disable IP-MAC binding for the switch	disable

Variable	Description	Default
l2-memory-check {enable   disable}	Enable or disable whether FortiSwitchOS checks the size of the layer-2 table. When this feature is enabled, the set l2-memory-check interval command controls the frequency that the table is checked. When the table size is more than 75-percent full or less than 70-percent full, FortiSwitchOS adds a warning to the system log.	disable
l2-memory-check-interval <number_of_seconds>	When l2-memory-check is enabled, FortiSwitchOS checks the size of the layer-2 table at the specified interval. The range of values is 5-86400 seconds.	120
log-mac-limit-violations {enable   disable}	Enable or disable the logging of layer-2 learning limit violations for an interface or VLAN. The most recent violation that occurred on each interface or VLAN is logged. After that, no more violations are logged until the log is reset for the triggered interface or VLAN. Only the most recent 128 violations are displayed in the console. <b>NOTE:</b> This command is only displayed if your FortiSwitch model supports it.	disable
log-source-guard-violations {enable   disable}	Enable or disable logs for source guard violations on a system-wide level.	disable
loop-guard-tx-interval <0-30>	Enter the loop guard transmit interval. Value range is 1-30. The units is seconds.	3
mac-aging-interval <seconds>	Specify how many seconds an unused MAC address is kept in the MAC table before being removed. The range is 10 to 1,000,000 seconds. Set to 0 to disable.	300
mac-violation-timer <integer>	How long (in minutes) violations of the layer-2 learning limit are kept in the log. The value range is 0-1500. Set to 0 to disable the timer.	0
max-frame-size <bytes_int>	Set the maximum frame size. The range and default depend on the switch model. See the FortiSwitchOS feature matrix. <b>NOTE:</b> If you are not using the FS-1xxE, FS-1xxF, or FS-110G-FPOE models, this command is under the config switch physical-port command.	Varies
max-path-in-ecmp-group <integer>	Set the maximum path in one ECMP group.	8
mclag-igmpsnooping-aware {enable   disable}	Enable this option to synchronize both query ports and group entries across peer MLAG trunks. This option can be used in standalone mode and in FortiLink mode. <b>NOTE:</b> For IGMP snooping to work correctly in an MLAG, you need to use the set mclag-igmpsnooping-aware enable command on all FortiSwitch units in the network topology and use the set igmps-flood-reports enable command on each MLAG core FortiSwitch unit.	disable

Variable	Description	Default
mclag-peer-info-timeout <integer>	Enter the MCLAG peer info timeout. The value range is 30 to 600 seconds.	30
mclag-port-base <integer>	Set the MCLAG port base.	0
mclag-split-brain-all-ports-down {enable   disable}	When this option is enabled and a split-brain state occurs, the switch that goes dormant shuts down all ports before going dormant; the state of the ICL trunk ports is not changed. When this option is disabled and a split-brain state occurs, the switch that goes dormant does not shut down any ports before going dormant. This command is only available when mclag-split-brain-detect is enabled.	disable
mclag-split-brain-detect {enable   disable}	Enable or disable the detection of the MCLAG split-brain state.	disable
mclag-split-brain-priority <0-100>	When the split-brain state occurs, the switch with the lowest priority goes dormant. If both switches have the same priority, the switch with the lowest MAC address goes dormant when the split-brain state occurs. This command is only available when mclag-split-brain-detect is enabled.	50
mclag-stp-aware {enable   disable}	Enable or disable whether the STP can be used within the MCLAG.	enable
mirror-qos <0-7>	Enter the quality of service (QoS) priority for packets mirrored by this FortiSwitch unit. Applies only to the FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE, FS-1048E, and FS-3032D models.	0
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 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 FS-1024D, FS-1048D, or FS-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-guard-band <integer>	Enter the power (W) to reserve in case of a spike in PoE consumption.	19

Variable	Description	Default
poe-power-budget <integer>	Set or override the maximum power budget.	400
poe-power-mode {first-come-first-served   priority}	Set the PoE power mode to priority based or first-come, first-served.	priority
poe-pre-standard-detect {disable   enable}	Enable or disable PoE pre-standard detection. <b>NOTE:</b> PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FS-548D-FPOE, FS-524D-FPOE, FS-108D-POE, FS-224D-POE, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, 148F-POE, and 148F-FPOE. For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.	disable
qos-drop-policy {random-early-detection   taildrop}	Set the CoS queue drop policy. <ul style="list-style-type: none"> <li>taildrop – When the queue is full, new packets are dropped.</li> <li>random-early-detection – As the queue fills, the probability increases that packets will be dropped.</li> </ul> <b>NOTE:</b> This command is available only for the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.	taildrop
qos-red-probability <integer>	Set the QoS RED/WRED drop probability. The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, and FS-124E-FPOE models support 0-100 percent. The FS-148E, FS-148E-POE, and FS-148E-FPOE models support 0-25 percent. <b>NOTE:</b> This command is available only for the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.	12
reserved-mcast-to-cpu {enable   disable}	Enable or disable the forwarding of IPv6 neighbor-discovery packets to the CPU. Applies only to the 200 Series and 400 Series.	enable
source-guard-violation-timer <integer>	Enter the number of minutes for a global timeout for source guard violations. The range of values is 0-1500. Set this option to 0 to disable it.  This command is only available when log-source-guard-violations is enabled.	0
storm-control-monitor {enable   disable}	Enable or disable storm-control monitoring.	disable
storm-control-high-rate <0-65536>	When this rate (in dropped packets per second) is exceeded, a log message is generated.  This command is only available when storm-control-monitor is enabled.	300

Variable	Description	Default
storm-control-rate-filter <0-100>	Set the percentage for how sensitive storm-control monitoring is to changes in the storm-control-high-rate. Higher percentages mean that the storm-control monitoring is more sensitive to changes in the storm-control-high-rate.  This command is only available when storm-control-monitor is enabled.	20
trunk-hash-mode {default  enhanced}	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   disable}	Enable or disable trunk hash for unknown unicast src-dst.	enable
virtual-wire-tpid <0x0001-0xfffe>	TPID value used by virtual-wires. The value range is from 0x0001 to 0xfffe.  Choose a value unlikely to be seen as a TPID or ethertype in your network.	0xdee5
vxlan-dport <integer >	Set the VXLAN destination UDP port. The range of values is 1-65535.	4789
vxlan-sport <integer>	Set the VXLAN source UDP port. The range of values is 1-65535.	0
vxlan-stp-virtual-mac <MAC_address>	Set the MAC address for the virtual STP root.  This option is available only when vxlan-stp-virtual-root is enabled.	08:5B:0E:00:00:00
vxlan-stp-virtual-root {enable   disable}	When this option is enabled, the local switch automatically becomes the STP root for STP instances that contain the configured VXLAN's access VLAN. When this option is disabled, the local switch does not automatically become the STP root for STP instances that contain the configured VXLAN's access VLAN.	disable
vxlan-qos-inner-to-outer {copy-to-outer   fixed}	Select how the differential service code point (DSCP) is determined: <ul style="list-style-type: none"> <li>copy-to-outer—Copy the DSCP value from the inner header to the outer header.</li> <li>fixed—Use a fixed DSCP value in the IP header of the outer encapsulation. Specify the fixed value with the set vxlan-qos-dscp command.</li> </ul>	copy-to-outer
vxlan-qos-dscp <0-63>	Specify the fixed DSCP value in the IP header of the outer encapsulation.  This command is available only when vxlan-qos-inner-to-outer is set to fixed.	0

Variable	Description	Default
<b>config port-security</b>		
link-down-auth	If a link goes down, this setting determines if the affected devices needs to reauthenticate. <ul style="list-style-type: none"> <li>set-unauth—revert all devices to the un-authenticated state. Each device will need to reauthenticate.</li> <li>no-action— if reauthentication is not required.</li> </ul>	set-unauth
mab-entry-as {dynamic   static}	Configure the MAC authentication bypass (MAB) MAC entries as static or dynamic: <ul style="list-style-type: none"> <li>In static mode, MAB sessions are kept until the link goes down or the MAB sessions are manually deleted with the CLI.</li> <li>In dynamic mode, MAB sessions are treated the same way as dynamically learned MAC addresses.</li> </ul>	static
mab-reauth {enable   disable}	Enable or disable whether MAB retries authentication before assigning a device to a guest VLAN for unauthorized users.	disable
mac-called-station-delimiter {colon   hyphen   none   single-hyphen}	Select which delimiter is used for the Called-Station-Id attribute or select none for no delimiter: <ul style="list-style-type: none"> <li>colon</li> <li>hyphen</li> <li>single-hyphen</li> </ul>	hyphen
mac-calling-station-delimiter {colon   hyphen   none   single-hyphen}	Select which delimiter is used for the Calling-Station-Id attribute or select none for no delimiter: <ul style="list-style-type: none"> <li>colon</li> <li>hyphen</li> <li>single-hyphen</li> </ul>	hyphen
mac-case {lowercase   uppercase}	Select whether MAC addresses use lowercase or uppercase letters.	lowercase
mac-password-delimiter {colon   hyphen   none   single-hyphen}	Select which delimiter is used for the User-Password attribute or select none for no delimiter: <ul style="list-style-type: none"> <li>colon</li> <li>hyphen</li> <li>single-hyphen</li> </ul>	hyphen
mac-username-delimiter {colon   hyphen   none   single-hyphen}	Select which delimiter is used for the User-Name attribute or select none for no delimiter: <ul style="list-style-type: none"> <li>colon</li> <li>hyphen</li> <li>single-hyphen</li> </ul>	hyphen
max-reauth-attempt	If 802.1x authentication fails, this setting caps the number of attempts that the system will initiate. The range is from 0 to 15 where "0" disables the reauthentication attempts.	3

Variable	Description	Default
quarantine-vlan {enable   disable}	Enable or disable quarantine VLAN detection. Enable this setting to use quarantines with 802.1x MAC-based authentication in FortiLink mode.	enable
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.	60
tx-period <12-60>	Specify how many seconds are allowed for the 802.1x reauthentication before it times out.	30

## 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 hsr ring

Use this command to configure a High-Availability Seamless Redundancy (HSR) ring.

### Syntax

```
config switch hsr ring
  edit {1 | 2}
    set status {enable | disable}
    set ring-port-pair <physical_port_pair>
    set redbox-mode hsr-san
    set vlan-id <1-4094>
    set vlan-id-cos <0-7>
    set vlan-id-tagged {enable | disable}
    set hsr-internal-vlan <VLAN_ID>
  next
end
```

Variable	Description	Default
status {enable   disable}	Enable or disable this HSR ring.	disable
ring-port-pair <physical_port_pair>	Select which port A and port B pair to use for this HSR ring. Enter set ring-port-pair ? to see the available physical port pairs.	No default
redbox-mode hsr-san	HSR-SAN is currently the only RedBox operation mode supported.	hsr-san
vlan-id <1-4094>	Enter the VLAN identifier of the supervision frame. This option is available only when vlan-id-tagged is set to enable.	1
vlan-id-cos <0-7>	Enter the class of service (CoS) value to be set in the VLAN tag of the supervision frame. This option is available only when vlan-id-tagged is set to enable.	0
vlan-id-tagged {enable   disable}	Enable or disable supervision frame VLAN ID tagging.	disable
hsr-internal-vlan <2-4094>	Assign all MAC addresses of this HSR ring to this internal VLAN ID. <b>NOTE:</b> If you are using an HSR ring and a PRP channel in your network, you need to change the default value so that each HSR ring and PRP channel is in a different internal VLAN.	No default

## Example

The following example configures an HSR ring:

```
config switch hsr ring
  edit 1
    set status enable
    set ring-port-pair port7-port8
  next
end
```

## config switch hsr settings

Use this command to configure HSR settings.

### Syntax

```
config switch hsr settings
  set mac-da <0-255>
  set life-check-interval <2-60 seconds>
end
```

Variable	Description	Default
mac-da <0-255>	Specify the last 8 bits of the HSR supervision frame MAC destination address (DA).	0
life-check-interval <2-60 seconds>	Specify how often (in seconds) the HSR supervision frame is generated for each MAC address in the VDAN table.	2

## Example

The following example configures the HSR settings:

```
config switch hsr settings
  set mac-da 100
  set life-check-interval 30
end
```

## config switch igmp-snooping globals

Use this command to configure global settings for IGMP snooping on the FortiSwitch unit.

### Syntax

```
config switch igmp-snooping globals
  set aging-time <1-20>
  set leave-response-timeout <integer>
  set lookup-mode {L2 | L3}
  set query-interval <10-1200>
  set query-max-response-timeout <100-32768>
end
```

Variable	Description	Default
aging-time <integer>	The maximum number of seconds to retain a multicast snooping entry for which no packets have been seen (15-3600).	300
leave-response-timeout <1-20>	Enter the maximum number of seconds that the switch waits after sending a group-specific query in response to the leave message.	10
lookup-mode {L2   L3}	Select whether IGMP groups are looked up by their IP addresses or their MAC addresses: <ul style="list-style-type: none"> <li>L2—Look up IGMP groups in the MAC address table. Set the lookup-mode to L2 for the FS-1024E, FS-T1024E, FS-T1024F-FPOE, FS-2048F, and FS-1048E models so that IGMP groups with TTL=1 streams are not dropped.</li> <li>L3—Look up IGMP groups in the IP multicast address table.</li> </ul>	L3

Variable	Description	Default
query-interval <10-1200>	Enter the maximum number of seconds between IGMP queries.	120
query-max-response-timeout <100-32768>	Enter the maximum number of milliseconds that a host waits for responses to a general query message.	10000

## Example

The following example configures global settings for IGMP snooping on the FortiSwitch unit:

```
config switch igmp-snooping globals
  set aging-time 150
  set leave-response-timeout 15
  set query-interval 200
end
```

## config switch interface

Use this command to configure FortiSwitch features on an interface.

**NOTE:** Settings under `config qnq` are for customer VLANs (C-VLANs). Other settings such as `set allowed-vlans`, `set native-vlan`, and `set vlan-tpid` are for service-provider VLANs (S-VLANs).

## Syntax

```
config switch interface
  edit <interface_name>
    set allowed-vlans {vlan1 vlan2 ...}
    set arp-inspection-trust {trusted | untrusted}
    set auto-discovery-fortilink-packet-interval <3-300>
    set default-cos <0-7>
    set description <string>
    set discard-mode {all-tagged | all-untagged | none}
    set dhcp-snooping {trusted | untrusted}
    set dhcp-snoop-learning-limit <1-16000>
    set dhcp-snoop-learning-limit-check {disable | enable}
    set dhcp-snooping-option82-trust {enable | disable}
    set edge-port {enabled | disabled}
    set force-egr-prio-tag {enable | disable}
    set igmp-snooping-flood-reports {enable | disable}
    set mcast-snooping-flood-traffic {enable | disable}
    set mld-snooping-flood-reports {enable | disable}
    set ip-mac-binding {enable | disable | global}
    set ip-source-guard {enable | disable}
    set learning-limit <0-128>
    set learning-limit-action {none | shutdown}
    set log-mac-event {enable | disable}
    set loop-guard {enabled | disabled}
    set loop-guard-timeout <0-120>
    set loop-guard-mac-move-threshold <0-100>
    set nac {enable | disable}
    set native-vlan <vlan_int>
```

```
set packet-sampler {enabled | disabled}
  set sample-direction {both | rx |tx}
set packet-sample-rate <0-99999>
set private-vlan {disabled | promiscuous sub-vlan}
set ptp-policy {<string> | default}
set ptp-status {enable | disable}
set qos-policy {<string> | default}
set rpvst-port {enabled | disabled}
set security-groups <security-group-name>
set sflow-counter-interval <0-255>
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 ...}
set vlan-mapping-miss-drop {enable | disable}
set vlan-tpid <default | string>
config dhcp-snoop-option82-override
  edit <VLAN_ID>
    set remote-id <string>
    set circuit-id <string>
  next
end
config port-security
  set {allow-mac-move-from | allow-mac-move-to} {enable | disable}
  set eap-egress-tagged {enable | disable}
  set port-security-mode {none | 802.1X | 802.1X-mac-based}
  set auth-fail-vlan {enable | disable}
  set auth-fail-vlanid <VLAN_id>
  set auth-order {MAB | MAB-dot1x | dot1x-MAB}
  set auth-priority {MAB-dot1x | dot1x-MAB | legacy}
  set authserver-timeout-period <3-15>
  set authserver-timeout-tagged {disable | lldp-voice | static}
  set authserver-timeout-tagged-vlanid <1-4094>
  set authserver-timeout-vlan {enable | disable}
  set authserver-timeout-vlanid <1-4094>
  set client-limit <2-20>
  set dacl {enable | disable}
  set eap-auto-untagged-vlans {enable | disable}
  set eap-passthru {disable | enable}
  set framevid-apply {disable | enable}
  set guest-auth-delay <integer>
  set guest-vlan {enable | disable}
  set guest-vlanid <VLAN_id>
  set mab-eapol-request <0-10>
  set mac-auth-bypass {enable | disable}
  set open-auth {enable | disable}
  set quarantine-vlan {enable | disable}
  set radius-timeout-override {enable | disable}
  next
end
config rguard
  edit <ID>
```

```

        set rguard-policy <name_of_RA_guard_policy>
        set vlan-list <list_of_VLANs>
    next
end
config qnq
    set status {enable | disable}
    set edge-type customer
    set vlan-mapping-miss-drop {enable | disable}
    set add-inner <1-4095>
    set remove-inner {enable | disable}
    set native-c-vlan <1-4094>
    set allowed-c-vlan <list_of_VLANs>
    set priority {follow-c-tag | follow-s-tag}
    set s-tag-priority <0-7>
    config vlan-mapping
        edit <id>
            set description <string>
            set match-c-vlan <1-4094>
            set new-s-vlan <1-4094>
        next
    end
end
config vlan-mapping
    edit <id>
        set description <string>
        set direction {egress | ingress}
        set match-s-vlan <1-4094>
        set match-c-vlan <1-4094>
        set action {add | delete | replace}
        set new-s-vlan <1-4094>
    next
end
next
end
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-packet- interval <3-300>	Enter the FortiLink packet interval for automatic discovery. The value range is 3 to 300 seconds.	5

Variable	Description	Default
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 <code>trust-dot1p-map</code> on the interface. <b>NOTE:</b> The set <code>default-cos</code> command is not available on the following FortiSwitch models: 224D-FPOE, 248D, 424D, 424D-POE, 424D-FPOE, 448D, 448D-POE, 448D-FPOE, 224E, 224E-POE, 248E-POE, and 248E-FPOE.	0
description <string>	Enter a description of the interface.	No default
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 <1-16000>	Set the maximum number of IP addresses learned on this interface for the DHCP-snooping binding database. The set <code>dhcp-snoop-learning-limit</code> command is available only when <code>dhcp-snoop-learning-limit-check</code> is enabled.	5
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
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
force-egr-prio-tag {enable   disable}	<b>NOTE:</b> This command is only for the FS-1xxE, FS-1xx, and FS-110G-FPOE models. Enable or disable the forced priority tagging on egress ports. <ul style="list-style-type: none"> <li><code>enable</code>—When the <code>allowed-vlans</code> command is set on a port, all egress traffic will have the priority tag of <code>vlan=0</code>. This command is most useful when the port is acting as an access port for native traffic only.</li> <li><code>disable</code>—Priority tagging is not forced on egress ports.</li> </ul>	disable
igmp-snooping-flood-reports {enable   disable}	Enable or disable whether to flood IGMP-snooping reports to this interface. <b>NOTE:</b> For IGMP snooping to work correctly in an MCLAG, you need to use the set <code>mclag-igmpsnooping-aware enable</code> command on all FortiSwitch units in the network topology and use the set <code>igmp-snooping-flood-reports enable</code> command on each MCLAG core FortiSwitch unit.	disable

Variable	Description	Default
mcast-snooping-flood-traffic {enable   disable}	Enable or disable whether to flood multicast traffic to this interface.	disable
mld-snooping-flood-reports {enable   disable}	Enable or disable whether to flood MLD-snooping reports 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
ip-source-guard {enable   disable}	Enable or disable IP source guard for this interface. After you enable this feature, use the <code>config switch ip-source-guard</code> command to configure it.	disable
learning-limit <0 - 128>	Limit the number of dynamic MAC addresses on this port.  The value range is 0 and 128. Setting the <code>learning-limit</code> to 0 means that there is no limit to the number of MAC addresses learned. <b>NOTE:</b> You cannot set the <code>learning-limit</code> on the internal interface.	0
learning-limit-action {none   shutdown}	When the <code>learning-limit</code> is exceeded, select <code>none</code> to take no action or select <code>shutdown</code> to disable this interface. The <code>learning-limit-action</code> applies only to physical switch port interfaces, not to trunks or VLANs.  The <code>learning-limit-action</code> is available only when <code>learning-limit</code> has been set to 1-128.	none
log-mac-event {enable   disable}	Enable or disable the logging of dynamic MAC address events.	disable
loop-guard {enabled   disabled}	Enable or disable loop guard for this interface.	disabled
loop-guard-timeout <0-120>	After enabling loop guard, set the number of minutes before loop guard resets. Setting this value to 0 means that there is no timeout.	45
loop-guard-mac-move-threshold <0-100>	After enabling loop guard, set the number of MAC address moves per second for this interface. The threshold must be exceeded for 6 consecutive seconds to trigger loop guard.	0
nac {enable   disable}	This command is available only in FortiLink mode. Enable to allow the switch to transmit MAC events to the FortiGate device to improve network access control (NAC) performance.	disable
native-vlan <vlan_int>	Enter the native (untagged) VLAN for this interface.	1
packet-sampler {enabled   disabled}	Enable or disable packet sampling for flow export.	disabled
sample-direction {both   rx   tx}	Set the sFlow sample direction to monitor received traffic (rx), monitor transmitted traffic (tx), or monitor both.  This option is only available when the <code>packet-sampler</code> is enabled.	both

Variable	Description	Default
packet-sample-rate <0-99999>	If packet-sampler is set to enabled, you can change the packet sample rate.	512
private-vlan {disabled   promiscuous   sub-vlan}	Enable private VLAN functionality. <b>NOTE:</b> Private VLANs are not supported on the FortiSwitch-28C.	disabled
ptp-policy {<string>   default}	Enter the name of the Precision Time Protocol (PTP) policy to apply to this port.	default
ptp-status {enable   disable}	Enable or disable PTP on this port.	enable
qos-policy {<string>   default}	Enter the name of the QoS egress CoS queue policy.	default
rpvst-port {enabled   disabled}	Enable or disable whether this interface interoperates with per-VLAN spanning tree (PVST).	disabled
security-groups <security-group-name>	Enter the security group name if you are using port-based authentication or MAC-based authentication.	No default
sflow-counter-interval <0-255>	Set the polling interval for the sFlow sampler counter. Set to 0 to disable polling.	0
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
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

Variable	Description	Default
vlan-mapping-miss-drop {enable   disable}	Enable or disable whether a packet is dropped if the VLAN ID in the packet's tag is not defined in the vlan-mapping configuration.	disable
vlan-tpid <default   string>	Select which VLAN TPID profile to use. The default VLAN TPID profile has a value of 0x8100 and cannot be deleted or changed. <b>NOTE:</b> If you are not using the default VLAN TPID profile, you must have already defined the VLAN TPID profile with the <code>config switch vlan-tpid</code> command.	default
<b>config dhcp-snoop-option82-override</b>		
<VLAN_ID>	Select the VLAN identifier.	No default
remote-id <string>	Enter the plain text string to use in the Remote ID field instead of the global value. The plain text string can be a maximum of 256 characters long. The combined length of the <code>remote-id</code> and <code>circuit-id</code> text strings can be a maximum of 256 characters long.	No default
circuit-id <string>	Enter the plain text string to use in the Circuit ID field instead of the global value. The plain text string can be a maximum of 256 characters long. The combined length of the <code>remote-id</code> and <code>circuit-id</code> text strings can be a maximum of 256 characters long.	No default
<b>config port-security</b>		
{allow-mac-move-from   allow-mac-move-to} {enable   disable}	Depending on the FortiSwitch model, you will see one of these commands: <ul style="list-style-type: none"> <li><code>allow-mac-move-from</code>—Enable on the source port when an 802.1x client is being moved between ports that are not directly connected to the FortiSwitch unit. This command is available only for the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.</li> <li><code>allow-mac-move-to</code>—Enable on the destination port when an 802.1x client is being moved between ports that are not directly connected to the FortiSwitch unit. This command is available only for FSR-124D, 200 Series, FS-4xxE, 500 Series, FS-1024D, FS-1024E, FS-T1024E, FS-1048E, and FS-3032E.</li> </ul>	disable
eap-egress-tagged {enable   disable}	When <code>allow-mac-move</code> is enabled, you can enable this option to ensure that egress EAPOL packets are tagged without needing additional checking.	enable
port-security-mode {none   802.1X   802.1X-mac-based}	Set the security mode for the port. <ul style="list-style-type: none"> <li><code>802.1X</code>—Use this setting for port-based authentication.</li> <li><code>802.1X-mac-based</code>—Use this setting for MAC-based authentication.</li> </ul> If you change the security mode to <code>802.1X</code> or <code>802.1X-mac-based</code> , you must set the security group with the <code>set security-groups</code> command.	none

Variable	Description	Default
auth-fail-vlan {enable   disable}	When enabled, the system assigns the <code>auth-fail-vlanid</code> to users who attempted to authenticate but failed to provide valid credentials.	disable
auth-fail-vlanid <VLAN_id>	Enter the VLAN identifier that the system assigns to users who attempted to authenticate but failed to provide valid credentials. This field is mandatory when <code>auth-fail-vlan</code> is enabled.	200
auth-order {MAB   MAB-dot1x   dot1x-MAB}	This command is available only when the <code>set mac-auth-bypass</code> command is enabled. Select one of the authentication order modes: <ul style="list-style-type: none"> <li><code>MAB</code>—In the MAB-only authentication mode, the FortiSwitch unit performs MAB authentication without performing EAP authentication. EAP packets are not sent.</li> <li><code>MAB-dot1x</code>—This command has been added for future use. It currently has no effect on authentication.</li> <li><code>dot1x-MAB</code>—This command has been added for future use. It currently has no effect on authentication.</li> </ul>	MAB-dot1x
auth-priority {MAB-dot1x   dot1x-MAB   legacy}	Select the priority of MAC authentication bypass (MAB) authentication and EAP 802.1X authentication. <ul style="list-style-type: none"> <li><code>MAB-dot1x</code>—The switch tries MAB authentication first and then EAP 802.1X authentication if MAB authentication fails. If EAP 802.1X authentication also fails, users are assigned to the <code>auth-fail-vlanid</code> VLAN if it is configured.</li> <li><code>dot1x-MAB</code>—The switch tries EAP 802.1X authentication first and then MAB authentication if EAP 802.1X fails. If MAB authentication also fails, users are assigned to the <code>auth-fail-vlanid</code> VLAN if it is configured.</li> <li><code>legacy</code>—The switch tries EAP 802.1X authentication and MAB authentication in the order that they are received with EAP 802.1X authentication having absolute priority. If authentication fails, users are assigned to a guest VLAN if it has been configured. There is no time delay involved.</li> </ul> This commands is available only when the <code>set mac-auth-bypass</code> command is enabled.	legacy
authserver-timeout-period <3-15>	Enter the number of seconds before the authentication server stops trying to authenticate users.	3
authserver-timeout-tagged {disable   lldp-voice   static}	Select whether users are assigned to the specified VLAN when the authentication server times out: <ul style="list-style-type: none"> <li><code>disable</code>—Users are not assigned to a specified VLAN when the authentication server times out.</li> <li><code>lldp-voice</code>—Users are assigned to the VLAN specified in the <code>set lldp-profile</code> command (under <code>config switch physical-port</code>).</li> <li><code>static</code>—Users are assigned to the tagged VLAN specified in the <code>set authserver-timeout-tagged-vlanid</code> command.</li> </ul>	disable

Variable	Description	Default
authserver-timeout-tagged-vlanid <1-4094>	Enter the identifier for the tagged VLAN that the system assigns to users when the authentication server times out.	300
authserver-timeout-vlan {enable   disable}	Enable or disable whether users are assigned to the specified VLAN when the authentication server times out.	disable
authserver-timeout-vlanid <1-4094>	Enter the identifier for the untagged VLAN that the system assigns to users when the authentication server times out. This field is mandatory when authserver-timeout-vlan is enabled.	300
client-limit <2-20>	Specify how many sessions are allowed on a port. This feature requires MAC-based 802.1X authentication and MAB.	20
dacl {enable   disable}	Enable or disable the dynamic access control list (DAACL) on this interface.	disable
eap-auto-untagged-vlans {enable   disable}	Enable to allow voice traffic with voice VLAN tag at egress.	enable
eap-passthru {disable   enable}	Enable or disable the EAP pass-through mode.	enable
frameid-apply {disable   enable}	Enable or disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN. <b>NOTE:</b> For phone and PC configuration only, disable frameid-apply to preserve the native VLAN when the data traffic is expected to be untagged.	enable
guest-auth-delay <integer>	If a device does not attempt to authenticate within this timeframe (in seconds), the guest VLAN is assigned.	5
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
mab-eapol-request <0-10>	Set how many EAP packets are sent to trigger EAP authentication for "silent supplicants" (such as end devices running Windows 7) that send non-EAP packets when they wake up from sleep mode. To disable this feature, set mab-eapol-request to 0 or disable mac-auth-bypass.	3
mac-auth-bypass {enable   disable}	Enable or disable MAC authentication bypass (MAB). If you enable MAB on the port, the system will use the device MAC address as the user name and password for authentication.	disable
open-auth {enable   disable}	Enable or disable open authentication (monitor mode) on this interface.	disable
quarantine-vlan {enable   disable}	Enable or disable quarantine VLAN detection. Enable this setting to use quarantines with 802.1x MAC-based authentication in FortiLink mode.	enable

Variable	Description	Default
radius-timeout-overwrite {enable   disable}	Enable this option to use the value of the session-timeout attribute. The session-timeout attribute specifies how many seconds of idleness are allowed before the FortiSwitch unit disconnects a session. The value must be more than 60 seconds.	disable
<b>config raguard</b>		
<ID>	Enter an identifier for the IPv6 RA-guard configuration.	No default
raguard-policy <name_of_RA_guard_policy>	Enter the name of the RA-guard policy to use for this interface. The RA-guard policy must be created (with the config switch raguard-policy command) before it is applied to an interface.	No default
vlan-list <list_of_VLANs>	Enter a VLAN or a range of VLANs to apply this policy to. Use less than 4,096 characters for the vlan-list value. Separate the VLANs and VLAN ranges with commas, for example: 1,3-4,6,7,9-100	All allowed VLANs on this port
<b>config qnq</b>		
status {enable   disable}	Enable this setting to use the VLAN stacking (QnQ) mode.	disable
edge-type customer	If the QnQ mode is enabled, the edge type is set to customer.	customer
vlan-mapping-miss-drop {enable   disable}	If the QnQ mode is enabled, enable or disable whether a frame is dropped if the VLAN ID in the frame's tag is not defined in the vlan-mapping configuration. This option is available only when allowed-c-vlan has not been set.	disable
add-inner <1-4095>	If the QnQ mode is enabled, add the inner tag for untagged frames upon ingress.	No default
remove-inner {enable   disable}	If the QnQ mode is enabled, enable or disable whether the inner tag is removed upon egress.	disable
native-c-vlan <1-4094>	Specify the native C VLAN (1-4094) for untagged packets. When you specify a value for native-c-vlan, FortiSwitchOS adds the native inner tag to untagged frames upon ingress and removes the native inner tag at egress.	No default
allowed-c-vlan <list_of_VLANs>	Specify single VLANs or ranges of VLANs. Use a comma to separate values without any spaces. The allowed-c-vlan applies to both ingress and egress. You must use less than 4,096 characters to list the VLANs. This option is available only when vlan-mapping-miss-drop is disabled.	No default
priority {follow-c-tag   follow-s-tag}	If the QnQ mode is enabled, select whether to follow the priority of the S-tag (service tag) or C-tag (customer tag). <b>NOTE:</b> This command is not available on the 224D-FPOE, 248D, 424D, 424D-POE, 424D-FPOE, 448D, 448D-POE, 448D-FPOE, 224E, 224E-POE, 248E-POE and 248E-FPOE models.	follow-s-tag
s-tag-priority <0-7>	If frames follow the priority of the S-tag (service tag), enter the priority value. This option is available only when the priority is set to follow-s-tag.	0

Variable	Description	Default
	<b>NOTE:</b> This command is not available on the 224D-FPOE, 248D, 424D, 424D-POE, 424D-FPOE, 448D, 448D-POE, 448D-FPOE, 224E, 224E-POE, 248E-POE and 248E-FPOE models.	
<b>config vlan-mapping (options available when QnQ is enabled)</b>		
<id>	Enter a mapping entry identifier.	No default
description <string>	Enter a description of the mapping entry.	No default
match-c-vlan <1-4094>	Enter a matching customer (inner) VLAN.	0
new-s-vlan <1-4094>	Enter a new service (outer) VLAN. <b>NOTE:</b> The VLAN must be in the port's allowed VLAN list. This option is only available after you set the value for match-c-vlan.	No default
<b>config vlan-mapping (options available when QnQ is disabled)</b>		
<id>	Enter an identifier for the VLAN mapping entry.	No default
description <string>	Enter a description of the VLAN mapping entry.	No default
direction {egress   ingress}	Select the ingress or egress direction.	No default
match-s-vlan <1-4094>	If the direction is set to egress, enter the service (outer) VLAN to match.	0
match-c-vlan <1-4094>	If the direction is set to ingress, enter the customer (inner) VLAN to match.	0
action {add   delete   replace}	Select what happens when the packet is matched: <ul style="list-style-type: none"> <li>• add—When the packet is matched, add the service VLAN. You cannot set the action to add for the egress direction.</li> <li>• delete—When the packet is matched, delete the service VLAN. You cannot set the action to delete for the ingress direction.</li> <li>• replace—When the packet is matched, replace the customer VLAN or service VLAN.</li> </ul> This option is only available after you set a value for match-c-vlan or match-s-vlan.	No default
new-s-vlan <1-4094>	Set the new service (outer) VLAN. This option is only available after you set the action to add or replace for the ingress direction or after you set the action to replace for the egress direction.	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
```

The following example shows how to configure 802.1x authentication:

```
config switch interface
  edit "port11"
    set native-vlan 200
    set snmp-index 11
    config port-security
      set port-security-mode 802.1X
      set auth-fail-vlan enable
      set auth-fail-vlanid 301
      set authserver-timeout-period 4
      set authserver-timeout-vlan enable
      set authserver-timeout-vlanid 300
      set eap-auto-untagged-vlans enable
      set eap-passthru enable
      set framevid-apply enable
      set guest-auth-delay 5
      set guest-vlan enable
      set guest-vlanid 401
      set mab-eapol-request 0
      set mac-auth-bypass disable
      set open-auth disable
      set quarantine-vlan enable
      set radius-timeout-overwrite enable
    end
  set security-groups "radius1grp"
  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 unit:

```
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 ip-source-guard

Use this command to configure IP source guard for a port by binding IPv4 addresses to MAC addresses.

### Syntax

```
config switch ip-source-guard
  edit <port_name>
    config binding-entry
      edit <id>
        set ip <xxx.xxx.xxx.xxx>
        set mac <XX:XX:XX:XX:XX:XX>
      next
    end
  next
end
```

Variable	Description	Default
<port_name>	Enter the name of the port.	No default
<id>	Enter a unique integer to create a new entry.	No default
ip <xxx.xxx.xxx.xxx>	Required. Enter the IPv4 address to bind to the MAC address. Masks are not supported.	0.0.0.0
mac <XX:XX:XX:XX:XX:XX>	Required. Enter the MAC address to bind to the IPv4 address.	00:00:00:00:00:00

## Example

The following example binds an IPv4 address to a MAC address so that traffic from that IP address will be allowed on port4:

```
config switch ip-source-guard
  edit port4
    config binding-entry
      edit 1
        set ip 172.168.20
        set mac 00:21:cc:d2:76:72
      next
    end
  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 | vlan-name}
    set 802.3-tlvs {eee-config | max-frame-size | power-negotiation}
    set auto-isl {enable | disable}
    set auto-isl-auth {legacy | strict | relax}
    set auto-isl-auth-encrypt {mixed | must | none}
    set auto-isl-auth-identity <string>
    set auto-isl-auth-macsec-profile default-macsec-auto-isl
    set auto-isl-auth-reauth <0-3600>
    set auto-isl-auth-user <string>
    set auto-isl-hello-timer <1-30>
    set auto-isl-port-group <0-9>
    set auto-isl-receive-timeout <3-90>
    set auto-mclag-icl {enable | disable}
    set med-tlvs (inventory-management | location-identification | network-policy | power-
      management)
    set vlan-name-map <single_VLANs_or_VLAN_ranges>
    config custom-tlvs
      edit <TLVname_str>
        set information-string <hex-bytes>
        set oui <hex-bytes>
        set subtype <integer>
      next
    config med-location-service
      edit address-civic
```

```

        set status {enable | disable}
        set sys-location-id <string>
    next
    edit coordinates
        set status {enable | disable}
        set sys-location-id <string>
    next
    edit elin-number
        set status {enable | disable}
        set sys-location-id <string>
    next
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 assign-vlan {enable | disable}
        set dscp <0 - 63>
        set priority <0 - 7>
        set vlan <0 - 4094>
    next
end

```

Variable	Description	Default
profile	Enter a name for the LLDP profile.	No default
802.1-tlvs {port-vlan-id   vlan-name}	The port-vlan-id TLV will send the native VLAN of the port. If the value is changed, the sent value will reflect the updated value.  The vlan-name TLV sends the VLAN descriptions that are configured in the set description command under config switch vlan.	No default
802.3-tlvs {eee-config   max-frame-size   power-negotiation}	Set which 802.3 TLVs are enabled: <ul style="list-style-type: none"> <li>• eee-config—Use this TLV to send the energy-efficient Ethernet (EEE) status of the port.</li> <li>• max-frame-size—This TLV will send the maximum frame size value of the port. If the value is changed, the sent value reflects the updated value.</li> <li>• power-negotiation—Use this TLV to send the power over Ethernet (PoE) classification of the port.</li> </ul>	no TLV enabled
auto-isl	Enable or disable the auto ISL capability.	Disabled
auto-isl-auth {legacy   strict   relax}	Select the authentication mode: <ul style="list-style-type: none"> <li>• legacy—This mode is the default. There is no authentication.</li> <li>• strict—If authentication succeeds, FortiOS forms a secure ISL trunk. If authentication fails, no ISL trunk is formed.</li> <li>• relax—If authentication succeeds, FortiOS forms a secure ISL trunk. If authentication fails, FortiOS forms a restricted ISL trunk.</li> </ul>	legacy

Variable	Description	Default
auto-isl-auth-encrypt {mixed   must   none}	<p>Select the encryption mode:</p> <ul style="list-style-type: none"> <li><b>mixed</b>—FortiOS enables MACsec on the ISL trunk ports that support MACsec; the ISL trunk members act as encrypted links. FortiOS disables MACsec on the ISL members that do not support MACsec; these ISL trunk members act as unencrypted links.</li> <li><b>must</b>—FortiOS enables MACsec on all ISL trunk members. If the port supports MACsec, the port acts as an encrypted link. If the port does not support MACsec, the port is removed from the ISL trunk, but the port still functions as a user port.</li> <li><b>none</b>—There is no encryption, and FortiOS does not enable MACsec on the ISL trunk members.</li> </ul> <p>This option is available when <code>auto-isl-auth</code> is set to <code>strict</code> or <code>relax</code>.</p>	none
auto-isl-auth-identity <string>	<p>Enter the identity, such as <code>fortilink</code>.</p> <p>This option is available when <code>auto-isl-auth</code> is set to <code>strict</code> or <code>relax</code>.</p>	No default
auto-isl-auth-macsec-profile default-macsec-auto-isl	<p>Use the <code>default-macsec-auto-isl</code> profile.</p> <p>This option is available when <code>auto-isl-auth-encrypt</code> is set to <code>mixed</code> or <code>must</code>.</p>	default-macsec-auto-isl
auto-isl-auth-reauth <0-3600>	<p>Enter the reauthentication period in minutes.</p> <p>This option is available when <code>auto-isl-auth</code> is set to <code>strict</code> or <code>relax</code>.</p>	3600
auto-isl-auth-user <string>	<p>Select the user certificate, such as <code>Fortinet_Factory</code>.</p> <p>This option is available when <code>auto-isl-auth</code> is set to <code>strict</code> or <code>relax</code>.</p>	No default
auto-isl-hello-timer <1-30>	<p>Enter a value (in seconds) for the hello timer. The range is 1 to 30.</p>	3
auto-isl-port-group <0-9>	<p>Enter a value for the port group. The range is 0 to 9.</p>	0
auto-isl-receive-timeout	<p>Enter a value (in seconds) for the receive timeout. The range is 3 to 90.</p>	9
auto-mclag-icl {enable   disable}	<p>Enable or disable the MCLAG inter-chassis link.</p>	disable
med-tlvs (inventory-management   location-identification   network-policy   power-management)	<p>Enable the inventory-management TLVs, location-identification TLVs, network-policy TLVs, and/or power-management TLVs.</p>	inventory-management network-policy location-identification
vlan-name-map <single_VLANs_or_VLAN_ranges>	<p>You can enter more than 10 VLAN identifiers, but only the first 10 VLANs with VLAN descriptions will be advertised.</p>	No default.

Variable	Description	Default
	<p>The VLAN identifiers are separated with commas and no spaces. The <code>vlan-name-map</code> configuration must be less than 4,096 characters.</p> <p>This option is available only when <code>802.1-tlvs</code> is set to <code>vlan-name</code>.</p>	
<b>config custom-tlvs</b>		
<code>&lt;TLVname_str&gt;</code>	Enter the TLV name.	No default
<code>information-string</code>	Organizationally defined information string. Enter up to 507 bytes in hexadecimal notation.	No default
<code>oui</code>	Organizationally unique identifier. Enter 3 hexadecimal bytes (000000 - FFFFFFF). At least one byte must have a non-zero value.	000000
<code>subtype</code>	Organizationally defined subtype. Enter an integer in the range of 0 to 255.	0
<b>config med-location-service</b>		
<code>address-civic</code>	Civic address and postal information.	No default
<code>status {enable   disable}</code>	Enable the status to transmit the type-length-value (TLV) if the LLDP-MED profile has been enabled on a port.	disable
<code>sys-location-id &lt;string&gt;</code>	Use the specified location entry that was already entered with the <code>config system location</code> command.	No default
<code>coordinates</code>	Coordinates of the location.	No default
<code>status {enable   disable}</code>	Enable the status to transmit the type-length-value (TLV) if the LLDP-MED profile has been enabled on a port.	disable
<code>sys-location-id &lt;string&gt;</code>	Use the specified location entry that was already entered with the <code>config system location</code> command.	No default
<code>elin-number</code>	Emergency location identifier number (ELIN).	No default
<code>status {enable   disable}</code>	Enable the status to transmit the type-length-value (TLV) if the LLDP-MED profile has been enabled on a port.	disable
<code>sys-location-id &lt;string&gt;</code>	Use the specified location entry that was already entered with the <code>config system location</code> command.	No default
<b>config med-network-policy</b>		
<code>{guest-voice   guest-voice-signaling   softphone-voice   streaming-video   video-conferencing   video-signaling   voice   voice-signaling}</code>	Enter one of the policy type names.	No default

Variable	Description	Default
status {enable   disable}	Enable or disable the policy for the policy type.	disable
assign-vlan {enable   disable}	Enable or disable whether the VLAN is added as one of the allowed-vlans for this port.	disable
dscp <0-63>	DSCP value to send.	0
priority <0-7>	CoS priority value to send.	0
vlan <0-4094>	VLAN value to send.  Setting this option to 0 will advertise the network policy as priority tagged, rather than VLAN tagged. Priority tagged network policies are always transmitted, whereas VLAN tagged are only transmitted if the VLAN is present on the switch interface sending the LLDP packet.	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>)
  set management-address {ipv4 | ipv6 | none}
  set device-detection {enable | disable}
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.	<b>mgmt</b> or <b>internal</b> , depending on FortiSwitch model.
management-address {ipv4   ipv6   none}	Select whether to advertise the IPv4 management address, the IPv6 management address, or no management address in the Management Address TLV	ipv4 ipv6
device-detection {enable   disable}	Enable or disable whether LLDP neighbor devices are dynamically detected. This option is available only in FortiLink mode.	disable

### 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
set management-address ipv4
end

```

## config switch macsec profile

Use these commands to configure a Media Access Control security (MACsec) profile.

### Syntax

```

config switch macsec profile
edit <profile_name>
  set cipher_suite {GCM-AES-128 | GCM-AES-256 | GCM-AES-XPB-128 | GCM-AES-XPB-256}
  set confident-offset {0 | 30 | 50}
  set eap-tls-ca-cert <CA_certificate>
  set eap-tls-cert <client_certificate>
  set eap-tls-identity <name_of_client>
  set eap-tls-radius-server <name_of_RADIUS_server>
  set encrypt-traffic {enable | disable}
  set include-macsec-sci {enable | disable}
  set include-mka-icv-ind enable
  set macsec-mode {static-cak | dynamic-cak}
  set macsec-validate strict
  set mka-priority <0-255>
  set mka-sak-rekey-time {0 | 60-1000000}
  set replay-protect {enable | disable}
  set replay-window <0-16777215>
  set status {enable | disable}
  config mka-psk
    edit <pre-shared key name>
      set crypto-alg {AES_128_CMAC | AES_256_CMAC}
      set mka-cak <string>
      set mka-ckn <string>
      set status active
    next
  end
  config traffic-policy
    edit <traffic_policy_name>
      set exclude-protocol {arp | dot1q | fortalink | ipv4 | ipv6 | lacp | lldp | qinq | stp}
      set security-policy must-secure
      set status enable
    next
  end
next
end

```

Variable	Description	Default
<profile_name>	Enter a name for the MACsec profile.	No default

Variable	Description	Default
cipher_suite {GCM-AES-128   GCM-AES-256   GCM-AES-XPN-128   GCM-AES-XPN-256}	Select which cipher suite to use for encryption.	GCM-AES-128
confident-offset {0   30   50}	Select the number of bytes for the MACsec traffic confidentiality offset. Selecting 0 means that all of the MACsec traffic is encrypted. Selecting 30 or 50 bytes means that the first 30 or 50 bytes of MACsec traffic are not encrypted.	0
eap-tls-ca-cert <CA_certificate>	Specify the certificate authority (CA) to use for the MACsec CAK. This option is available only when macsec-mode is set to dynamic-cak.	No default
eap-tls-cert<client_certificate>	Select the client certificate that you imported for the MACsec CAK. This option is available only when macsec-mode is set to dynamic-cak.	No default
eap-tls-identity <name_of_client>	Enter the name of the client for the MACsec CAK. This option is available only when macsec-mode is set to dynamic-cak.	No default
eap-tls-radius-server <name_of_RADIUS_server>	Enter the name of the RADIUS server to use for the MACsec CAK. This option is available only when macsec-mode is set to dynamic-cak.	No default
encrypt-traffic {enable   disable}	Enable or disable whether MACsec traffic is encrypted.	enable
include-macsec-sci {enable   disable}	Enable or disable whether to include the MACsec transmit secure channel identifier (SCI).	enable
include-mka-icv-ind enable	The MACsec Key Agreement (MKA) integrity check value (ICV) indicator is always included.	enable
macsec-mode {static-cak   dynamic-cak}	Select whether MACsec uses the static-CAK mode or the dynamic-CAK mode.	static-cak
macsec-validate strict	The MACsec validation is always strict.	strict
mka-priority <0-255>	Enter the MACsec MKA priority.	255
mka-sak-rekey-time{0   60-1000000}	Set the number of seconds before a new secure association key (SAK) is generated. Set to 0 to disable the timer. The minimum number of seconds is 60; the maximum number of seconds is 1,000,000.	0
replay-protect {enable   disable}	Enable or disable MACsec replay protection. MACsec replay protection drops packets that arrive out of sequence, depending on the replay-window value.	disable

Variable	Description	Default
replay-window <0-16777215>	Enter the number of packets for the MACsec replay window size. If two packets arrive with the difference between their packet identifiers more than the replay window size, the most recent packet of the two is dropped. The range is 0-16777215 packets. Enter 0 to ensure that all packets arrive in order without any repeats.	32
status {enable   disable}	Enable or disable this MACsec profile.	enable
<b>config mka-psk</b>	Configure the MACsec MKA pre-shared key.	
<pre-shared key name>	Enter a name for this MACsec MKA pre-shared key configuration.	No default
crypto-alcrypto-alg {AES_128_CMAC   AES_256_CMAC}	Select the AES_128_CMAC or AES_256_CMAC algorithm to encrypt the pre-shared key.	AES_128_CMAC
mka-cak <string>	Enter the string of hexadecimal digits for the connectivity association key (CAK). The string can be up to 32-bytes or 64-bytes long.	No default
mka-ckn <string>	Enter the string of hexadecimal digits for the connectivity association name (CKN). The string must be an even number of bytes, 2-bytes to 64-bytes long.	No default
status active	The status of the pre-shared key pair is always active.	active
<b>config traffic-policy</b>	Configure the MACsec traffic policy.	
<traffic_policy_name>	Enter a name for this MACsec traffic policy.	No default
exclude-protocol {arp   dot1q   fortalink   ipv4   ipv6   lacp   lldp   qinq   stp}	Select one or more protocols that will not be secured by the MACsec traffic policy: <ul style="list-style-type: none"> <li>arp—Do not encrypt ARP packets.</li> <li>dot1q—Do not encrypt 802.1q VLAN packets.</li> <li>fortalink—Do not encrypt FortiLink packets.</li> <li>ipv4—Do not encrypt IPv4 packets.</li> <li>ipv6—Do not encrypt IPv6 packets.</li> <li>lacp—Do not encrypt LACP packets.</li> <li>lldp—Do not encrypt LLDP packets.</li> <li>qinq—Do not encrypt 802.1ad QinQ packets.</li> <li>stp—Do not encrypt STP packets.</li> </ul> Separate protocols with a space. By default, all protocols are encrypted if no protocols are excluded.	No default
security-policy must-secure	The policy must secure traffic for MACsec.	must-secure
status enable	The status of this MACsec traffic policy is always enabled.	enable

## Example

This example configures a MACsec profile.

```
config switch macsec profile
```

```
edit "2"
  set cipher_suite GCM-AES-128
  set confident-offset 0
  set encrypt-traffic enable
  set include-macsec-sci enable
  set include-mka-icv-ind enable
  set macsec-mode static-cak
  set macsec-validate strict
  set mka-priority 199
  config mka-psk
    edit "2"
      set crypto-alg AES_128_CMAC
      set mka-cak "0123456789ABCDEF0123456789ABCDEE"
      set mka-ckn "6162636465666768696A6B6C6D6E6F707172737475767778797A303132333436"
      set status active
    next
  end
  set replay-protect disable
  set replay-window 32
  set status enable
  config traffic-policy
    edit "2"
      set security-policy must-secure
      set status enable
    next
  end
next
end
```

## config switch mirror

Use these commands to configure the packet mirror. Packet mirroring allows you to collect packets on specified ports and then send them to another port to be collected and analyzed.

### Syntax

```
config switch mirror
  edit <mirror session name>
    set dst <interface>
    set encap-gre-protocol <hexadecimal_integer>
    set encap-ipv4-src <IPv4_address>
    set encap-ipv4-tos <hexadecimal_integer>
    set encap-ipv4-ttl <0-255>
    set encap-mac-dst <MAC_address>
    set encap-mac-src <MAC_address>
    set encap-vlan {tagged | untagged}
    set encap-vlan-cfi <0-1>
    set encap-vlan-id <1-4094>
    set encap-vlan-priority <0-7>
    set encap-vlan-tpid <0x0001-0xfffe>
    set erspan-collector-ip <IPv4_address>
    set mode {ERSPAN-auto | ERSPAN-manual | RSPAN | SPAN}
    set rspan-ip <IPv4_address>
    set src-egress <interface_name>
```

```

set src-ingress <interface_name>
set status {active | inactive}
set strip-mirrored-traffic-tags {disable | enable}
set switching-packet {enable | disable}
end

```

Variable	Description	Default
<mirror session name>	Enter the name of the mirror session to edit (or enter a new mirror session name).	No default
dst <interface>	<p>Required when the mode is set to ERSPAN-manual, RSPAN (when the switch is not in FortiLink mode), or SPAN.</p> <p>On FortiSwitch models that support RSPAN and ERSPAN, set the trunk or physical port that will act as a mirror. The physical port cannot be part of a trunk.</p> <p>On FortiSwitch models that do <i>not</i> support RSPAN and ERSPAN, set the physical port that will act as a mirror. The physical port can be part of a trunk.</p>	No default
encap-gre-protocol <hexadecimal_integer>	<p>Set the protocol value in the ERSPAN GRE header.</p> <p>This option is available when the mode is ERSPAN-auto or ERSPAN-manual.</p>	0x88be
encap-ipv4-src <IPv4_address>	<p>Required when the mode is set to ERSPAN-manual and the status is active.</p> <p>Set the IPv4 source address in the ERSPAN IP header. The range is 0.0.0.1-255.255.255.254.</p> <p>This option is available when the mode is ERSPAN-manual.</p>	0.0.0.0
encap-ipv4-tos <hexadecimal_integer>	<p>Set the type of service (ToS) value or enter the DSCP and ECN values in the ERSPAN IP header.</p> <p>This option is available when the mode is ERSPAN-auto or ERSPAN-manual.</p>	0x00
encap-ipv4-ttl <0-255>	<p>Set the IPv4 time-to-live (TTL) value in the ERSPAN IP header.</p> <p>This option is available when the mode is ERSPAN-auto or ERSPAN-manual.</p>	16
encap-mac-dst <MAC_address>	<p>Required when the mode is set to ERSPAN-manual and the status is active.</p> <p>Set the MAC address of the next-hop or gateway on the path to the ERSPAN collector IP address. The range is 00:00:00:00:00:01-FF:FF:FF:FF:FF:FF.</p> <p>This option is available only when the mode is ERSPAN-manual.</p>	00:00:00:00:00:00

Variable	Description	Default
encap-mac-src <MAC_address>	<p>Required when the mode is set to ERSPAN-manual and the status is active.</p> <p>Set the source MAC address in the ERSPAN Ethernet header. The range is 00:00:00:00:00:01-FF:FF:FF:FF:FF:FE.</p> <p>This option is available when the mode is ERSPAN-manual.</p>	00:00:00:00:00:00
encap-vlan {tagged   untagged}	<p>Set the status of ERSPAN encapsulation headers to tagged or untagged to control whether the VLAN header is added to the encapsulated traffic.</p> <p>This option is available if the mode is ERSPAN-manual.</p>	untagged
encap-vlan-cfi <0-1>	<p>Set the canonical format identifier (CFI) or drop eligible indicator (DEI) bit in the ERSPAN or RSPAN VLAN header.</p> <p>This option is available when the mode is RSPAN or ERSPAN-auto. This option is available for the ERSPAN-manual mode if encap-vlan is set to tagged.</p> <p>When the mode is RSPAN, this option is not available on the 248D, 248D-POE, 248D-FPOE, 248E, 248E-POE, 248E-FPOE, 448D, 448D-POE, and 448D-FPOE models.</p>	0
encap-vlan-id <1-4094>	<p>Set the VLAN identifier in the ERSPAN or RSPAN VLAN header.</p> <p>This option is available when the mode is RSPAN. This option is available for the ERSPAN-manual mode if encap-vlan is set to tagged.</p>	1
encap-vlan-priority <0-7>	<p>Set the class of service (CoS) bits in the ERSPAN or RSPAN VLAN header.</p> <p>This option is available when the mode is RSPAN or ERSPAN-auto. This option is available for the ERSPAN-manual mode if encap-vlan is set to tagged.</p> <p>When the mode is RSPAN, this option is not available on the 248D, 248D-POE, 248D-FPOE, 248E, 248E-POE, 248E-FPOE, 448D, 448D-POE, and 448D-FPOE models.</p>	0
encap-vlan-tpid <0x0001-0xffff>	<p>Set the tag protocol identifier (TPID) for the encapsulating VLAN header. The default value, 0x8100, is for an IEEE 802.1Q-tagged frame.</p> <p>This option is available when the mode is RSPAN or ERSPAN-auto. This option is available for the ERSPAN-manual mode if encap-vlan is set to tagged.</p>	0x8100

Variable	Description	Default
erspan-collector-ip <IPv4_address>	<p>Required when the status is active and the mode is set to ERSPAN-auto or ERSPAN-manual.</p> <p>Set the IPv4 address for the ERSPAN collector. The range is 0.0.0.1-255.255.255.255.</p> <p>This option is available only when the mode is ERSPAN-auto or ERSPAN-manual.</p>	0.0.0.0
mode {ERSPAN-auto   ERSPAN-manual   RSPAN   SPAN}	<p>Select the mirroring mode:</p> <ul style="list-style-type: none"> <li>ERSPAN-auto—Mirror traffic to the specified destination interface using ERSPAN encapsulation. The header contents are automatically configured.</li> <li>ERSPAN-manual—Mirror traffic to the specified destination interface using ERSPAN encapsulation. The header contents are manually configured.</li> <li>RSPAN—Mirror traffic to the specified destination interface using RSPAN encapsulation.</li> <li>SPAN—Mirror traffic to the specified destination interface without encapsulation.</li> </ul> <p>SPAN is supported on all FortiSwitch models. RSPAN and ERSPAN are supported on 124D, 224D-FPOE, 248D, 424D, 424D-POE, 424D-FPOE, 448D, 448D-POE, 448D-FPOE, 224E, 224E-POE, 248E-POE, 248E-FPOE, 524D, 524D-FPOE, 548D, 548D-FPOE, 1024D, 1048D, 1048E, 3032D, and 3032E.</p>	SPAN
rspan-ip <IPv4_address>	<p>Required when the mode is RSPAN, the status is active, and the switch is in FortiLink mode.</p> <p>Enter the destination IP address for the RSPAN collector. The range is 0.0.0.1-255.255.255.255.</p> <p>This option is available only when the mode is RSPAN and the switch is in FortiLink mode.</p>	0.0.0.0
src-egress <interface_name>	Optional. Set the source egress physical ports that will be mirrored. Only one active egress mirror session is allowed.	No default
src-ingress <interface_name>	Optional. Specify the source ingress physical ports that will be mirrored.	No default
status {active   inactive}	Set the mirror session to active or inactive.	inactive
strip-mirrored-traffic-tags {disable   enable}	<p>Enable or disable the removal of VLAN tags from mirrored traffic.</p> <p>This option is available if the mode is ERSPAN-auto or ERSPAN-manual.</p>	disable
switching-packet {enable   disable}	Enable or disable the switching functionality on the dst interface when mirroring.	disable

## Example

The following example configures a port mirror:

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

## config switch mld-snooping globals

Use this command to configure global settings for Multicast Listener Discovery (MLD) snooping on the FortiSwitch unit.

### Syntax

```
config switch mld-snooping globals
  set aging-time <integer>
  set leave-response-timeout <integer>
  set query-interval <10-1200>
end
```

Variable	Description	Default
aging-time <integer>	The maximum number of seconds to retain a multicast snooping entry for which no packets have been seen (15-3600).	300
leave-response-timeout <integer>	Enter the maximum number of seconds that the switch waits after sending a group-specific query in response to the leave message. The range of values is 1-20.	10
query-interval <10-1200>	Enter the maximum number of seconds between MLD queries.	125

### Example

The following example configures the global settings for MLD snooping on the FortiSwitch unit:

```
config switch mld-snooping globals
  set aging-time 150
  set leave-response-timeout 15
  set query-interval 200
end
```

## config switch mrp profile

Use this command to configure a Media Redundancy Protocol (MRP) profile.

## Syntax

```
config switch mrp profile
  edit <MRP_profile_name>
    set default-test-interval <30-50 ms>
    set short-test-interval <10-30 ms>
    set test-monitoring-count <1-5>
    set topology-change-interval <10-20 ms>
    set topology-change-repeat-count <1-5>
  next
end
```

Variable	Description	Default
<MRP_profile_name>	Enter a name for the MRP profile.	No default
default-test-interval <30-50 ms>	Enter the default number of milliseconds between sending MRP_Test frames.	50
short-test-interval <10-30 ms>	Enter the number of milliseconds before sending MRP_Test frames after link changes in the ring.	30
test-monitoring-count <1-5>	Enter the number of MRP_Test frames received that are monitored.	5
topology-change-interval <10-20 ms>	Enter the number of milliseconds between sending MRP_TopologyChange frames.	20
topology-change-repeat-count <1-5>	Enter the number of repeated MRP_TopologyChange frames that are transmitted.	3

## config switch mrp settings

Use this command to configure the Media Redundancy Protocol (MRP) settings.

### Syntax

```
config switch mrp settings
  edit <MRP_ring_ID>
    set status {disable | enable}
    set role {automanager | client}
    set domain-id <32_hexadecimal_digits>
    set domain-name <domain_name>
    set vlan-id <1-4094>
    set priority <0-65535>
    set ring-port1 <port_name>
    set ring-port2 <port_name>
    set profile-name {500ms | <custom_profile_name>}
  next
end
```

Variable	Description	Default
<MRP_ring_ID>	Enter a unique identifier for this MRP ring.	No default
status {disable   enable}	Enable or disable MRP.	disable
role {automanager   client}	Select whether the switch acts as an MRP client or an MRP automanager.	client
domain-id <32_hexadecimal_digits>	Enter a universally unique identifier to represent the MRP ring.	FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF
domain-name <domain_name>	Enter a unique logical name for the MRP domain identifier.	domain1
vlan-id <1-4094>	Optional. Enter the VLAN identifier for sending MRP frames. If you set this option to a different value than 1, the VLAN must be created before it is assigned to the MRP ring.	1
priority <0-65535>	Enter the priority of the MRP manager. The highest priority is 0, and the lowest priority is 65535.	40960
ring-port1 <port_name>	The physical port that serves as the first ring port.	No default
ring-port2 <port_name>	The physical port that serves as the second ring port.	No default
profile-name {500ms   <custom_profile_name>}	A unique MRP profile name.	500ms

## Example

This example shows how to configure the settings for the MRP manager:

```
config switch mrp settings
  edit 1
    set status enable
    set role automanager
    set domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF
    set domain-name domain1
    set vlan-id 4094
    set priority 40960
    set ring-port1 port7
    set ring-port2 port8
    set profile-name profile1
  next
end
```

## config switch network-monitor directed

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

## 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 unit.

## Syntax

```
config switch network-monitor settings
  set db-aging-interval <3600-86400>
  set status {disable | enable}
  set survey-mode {disable | enable}
  set survey-mode-interval <120-3600>
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

Use this command to configure split ports or to set the speed of the FS-2048F ports.

### Syntax

```

config switch phy-mode
  set port-configuration {default | disable-port54 | disable-port41-48 | 4x100G | 6x40G | 4x4x25G}
  set {<port-name>-phy-mode <single-port> | port1-port12-phy-mode | port13-port24-phy-mode |
      port25-port36-phy-mode | port37-port48-phy-mode} {4x25G | 4x10G | 4x1G | 2x50G | 1G/10G |
      25G}
  ...
end

```

Variable	Description	Default
port-configuration {default   disable-port54   disable-port41-48   4x100G   6x40G   4x4x25G}	<ul style="list-style-type: none"> <li>For 548D and 548D-FPOE, set this option to <code>disable-port54</code> if only port 53 is splittable and port 54 is unavailable.</li> <li>For 548D and 548D-FPOE, set this option to <code>disable-port41-48</code> if ports 41 to 48 are unavailable, but ports 53 and 54 are splittable.</li> <li>For 1048E, set this option to <code>4x100G</code> to enable the maximum speed (100G) of ports 49 through 52. Ports 53 and 54 are disabled.</li> <li>For 1048E, set this option to <code>6x40G</code> to enable the maximum speed (40G) of ports 49 through 54.</li> <li>For 1048E, set this option to <code>4x4x25G</code> to enable the maximum speed (25G) of ports 49 through 52. Ports 47 and 48 are disabled.</li> </ul>	default
{<port-name>-phy-mode <single-port>   port1-port12-phy-mode   port13-port24-phy-mode   port25-port36-phy-mode   port37-port48-phy-mode} {4x25G   4x10G   4x1G   2x50G   1G/10G   25G}	<p>Use one entry for each port that supports split ports.</p> <ul style="list-style-type: none"> <li>Set this option to <code>single-port</code> to use the port at the full base speed without splitting it.</li> <li>For FS-2048F, set this option to <code>port1-port12-phy-mode</code> to set the speed of ports 1-12.</li> <li>For FS-2048F, set this option to <code>port13-port24-phy-mode</code> to set the speed of ports 13-24.</li> <li>For FS-2048F, set this option to <code>port25-port36-phy-mode</code> to set the speed of ports 25-36.</li> <li>For FS-2048F, set this option to <code>port37-port48-phy-mode</code> to set the speed of ports 37-48.</li> </ul>	1x40G

Variable	Description	Default
	<ul style="list-style-type: none"> <li>For 100G QSFP only, set this option to 4x25G to split one port into four subports of 25 Gbps each. <b>NOTE:</b> For the FS-T1024E and FS-1024E models, detect-by-module selects the correct speed for the subports. If you insert a 100G QSFP28 module, the subports are automatically changed to 4x25G. If you insert a 40G QSFP+ module, the subports are automatically changed to 4x10G.</li> <li>For 40G or 100G QSFP only, set this option to 4x10G to split one port into four subports of 10Gbps each.</li> <li>For 40G or 100G QSFP only, set this option to 4x1G to split one port into four subports of 1 Gbps each.</li> <li>For 100G QSFP only, set this option to 2x50G to split one port into two subports of 50 Gbps each.</li> <li>For FS-2048F, set this option to 1G/10G to set the speed of the ports to 1G or 10G.</li> <li>For FS-2048F, set this option to 25G to set the speed of the ports to 25G.</li> </ul>	

## 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
```

In the following example, a FortiSwitch 1048E model is configured so that each port is split into four subports of 25 Gbps each.

```
config switch phy-mode
  set port-configuration 4x4x25G
  set port49-phy-mode 4x25G
  set port50-phy-mode 4x25G
  set port51-phy-mode 4x25G
  set port52-phy-mode 4x25G
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 energy-efficient-ethernet {enable | disable}
    set eee-tx-idle-time <integer>
    set eee-tx-wake-time <integer>
    set fec-state {c174 | c191 | detect-by-module | disabled}
    set flapguard {enabled | disabled}
    set flap-duration <5-300>
    set flap-rate <1-30>
    set flap-timeout <0-120>
    set flow-control {tx | rx | both | disable}
    set fortilink-p2p {enable | disable}
    set pause-meter-rate <integer>
    set pause-resume {25% | 50% | 75%}
    set l2-learning {enable | disable}
    set l2-sa-unknown {drop | forward}
    set lldp-profile <profile name>
    set lldp-status {tx-only | rx-only | tx-rx | disable}
    set loopback {disable | local | remote}
    set macsec-pae-mode {none | supp | auth}
    set macsec-profile <string>
    set max-frame-size <bytes_int>
    set poe-disconnection-type {AC | DC | DC-delay}
    set poe-max-power-mode {30W | 60W | class-based}
    set poe-port-mode {IEEE802_3AF | IEEE802_3AT}
    set poe-port-power {normal | perpetual | perpetual-fast}
    set poe-port-priority {critical-priority | high-priority | low-priority}
    set poe-pre-standard-detect {disable | enable}
    set poe-status {enable | disable}
    set priority-based-flow-control {enable | disable}
    set qsfp-low-power-mode {enabled | disabled}
    set security-mode {none | macsec}
    set speed <speed_str>
    set status {down | up}
```

```

set storm-control-mode {disabled | global | override}
config storm-control
  set broadcast {enable | disable}
  set burst-size-level <0-4>
  set rate [0 | 2-10000000]
  set unknown-multicast {enable | disable}
  set unknown-unicast {enable | disable}
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). <ul style="list-style-type: none"> <li>• disable disables CDP transmit and receive.</li> <li>• rx-only enables CDP as receive only.</li> <li>• tx-only enables CDP as transmit only.</li> <li>• tx-rx enables CDP transmit and receive.</li> </ul>	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
energy-efficient-ethernet {enable   disable}	Enable or disable energy-efficient Ethernet.	disable
eee-tx-idle-time <integer>	Enter the number of microseconds that circuits are turned off to save power. The range is 0-2560 microseconds. This option is available only if energy-efficient-ethernet is enabled.	60
eee-tx-wake-time <integer>	Enter the number of microseconds during which no data is transmitted while the circuits that were turned off are being restarted. The range is 0-2560 microseconds. This option is available only if energy-efficient-ethernet is enabled.	30
fec-state {cl74   cl91   detect-by-module   disabled}	Set the Forward Error Correction (FEC) state: <ul style="list-style-type: none"> <li>• cl74—Enable Clause 74 RS-FEC, which only applies to 25 Gbps.</li> <li>• cl91—Enable Clause 91 RS-FEC, which only applies to 100 Gbps.</li> <li>• detect-by-module—Automatically detect whether FEC is supported by the module. This option applies to the 25G and 100G ports of the FS-1048E and FS-3032E models; this option also applies to the split ports of the FS-1048E and FS-3032E models.</li> <li>• disabled—Disable FEC.</li> </ul>	detect-by-module
flapguard {enabled   disabled}	Enable or disable flap guard for this port.	disabled

Variable	Description	Default
flap-duration <5-300>	After enabling the port flap guard, set the number of seconds during which the flap rate is counted.	30
flap-rate <1-30>	After enabling the port flap guard, set how many times that a port's status changes during a specified number of seconds before the flap guard is triggered.	5
flap-timeout <0-120>	After enabling the port flap guard, set the number of minutes before flap guard resets. Setting this value to 0 means that there is no timeout.	0
flow-control {tx   rx   both   disable}	Set flow control: <ul style="list-style-type: none"> <li>tx—Enable transmit pause only.</li> <li>rx—Enable receive pause only.</li> <li>both—Enable both transmit and receive pause.</li> <li>disable—Disable flow control.</li> </ul>	disable
fortilink-p2p {enable   disable}	Enable or disable running FortiLink mode over a point-to-point layer-2 network.	disable
pause-meter-rate <integer>	Enter the number of kilobits for the ingress metering rate. The range is 64 to 2147483647. Set to 0 to disable. Available if flow-control is set to tx.	0
pause-resume {25%   50%   75%}	Enter the percentage of the threshold to resume traffic to the ingress port. Available if flow-control is set to tx and pause-meter-rate is set to a nonzero value.	75%
l2-learning	Enable or disable dynamic IP learning for this interface	enabled
l2-sa-unknown {drop   forward}	Drop or forward unknown (SMAC) packets when dynamic MAC address learning is disabled.	drop
lldp-profile	Enter the LLDP profile name for this port.	default
lldp-status	Set LLDP status for this port: <ul style="list-style-type: none"> <li>tx-only—enable transmit only</li> <li>rx-only—enable receive only</li> <li>tx-rx—enable both transmit and receive</li> <li>disable—disable LLDP</li> </ul>	tx-rx
loopback {disable   local   remote}	Set whether the physical port loops back on itself, either locally or remotely: <ul style="list-style-type: none"> <li>Select local for a physical-layer loopback. If the hardware does not support a physical-layer loopback, a MAC-address loopback is used instead.</li> <li>Select remote for a physical-layer lineside loopback.</li> </ul>	disable
macsec-pae-mode {none   supp   auth}	Select the PAE mode for the MACSEC interface: <ul style="list-style-type: none"> <li>none—No PAE is configured, and PSK is applied.</li> <li>supp—The interface acts as a PAE supplicant for MACsec CAK.</li> </ul>	none

Variable	Description	Default
	<ul style="list-style-type: none"> <li><code>auth</code>—The interface acts as a PAE authenticator for MACsec CAK.</li> </ul>	
<code>macsec-profile &lt;string&gt;</code>	Specify the MACsec profile to apply to the port.	No default
<code>max-frame-size &lt;bytes_int&gt;</code>	<p>Set the maximum frame size. The range and default depend on the switch model. See the FortiSwitchOS feature matrix.</p> <p><b>NOTE:</b> For the FS-1xxE, FS-1xxF, and FS-110G-FPOE models, this command is under the <code>config switch global</code> command.</p>	Varies
<code>poe-disconnection-type {AC   DC   DC-delay}</code>	<p>Select how a FortiSwitch unit with Power over Ethernet (PoE) disconnects from a powered device:</p> <ul style="list-style-type: none"> <li><code>AC</code>—AC disconnect.</li> <li><code>DC</code>—DC disconnect.</li> <li><code>DC-delay</code>—DC disconnect with an extra 500-millisecond delay.</li> </ul>	DC
<code>poe-max-power-mode {30W   60W   class-based}</code>	<p>Set the maximum amount of power on PoE ports to 30 W, 60 W, or the maximum amount of power for that port:</p> <ul style="list-style-type: none"> <li><code>30W</code>—The maximum amount of power on this port is 30 W.</li> <li><code>60W</code>—The maximum amount of power on this port is 60 W.</li> <li><code>class-based</code>—The maximum amount of power on this port is based on the class.</li> </ul>	class-based
<code>poe-port-mode {IEEE802_3AF   IEEE802_3AT}</code>	Set the PoE port mode to IEEE802.3AF or IEEE802.3AT.	IEEE802_3AT
<code>poe-port-power {normal   perpetual   perpetual-fast}</code>	<p>Select whether the PoE power is delivered while a switch restarts:</p> <ul style="list-style-type: none"> <li><code>normal</code>—PoE power is not provided while a switch restarts.</li> <li><code>perpetual</code>—PoE power is provided during a soft reboot (switch is restarted while powered up).</li> <li><code>perpetual-fast</code>—PoE power is provided during a hard reboot (the switch's power is physically turned off and then on again).</li> </ul>	normal
<code>poe-port-priority {critical-priority   high-priority   low-priority}</code>	Set the port priority. If there is not enough power, power is allotted first to critical-priority ports, then to high-priority ports, and then to low-priority ports.	low-priority
<code>poe-pre-standard-detect {disable   enable}</code>	<p>Enable or disable PoE pre-standard detection.</p> <p><b>NOTE:</b> PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FS-548D-FPOE, FS-524D-FPOE, FS-108D-POE, FS-224D-POE, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, 148F-POE, and 148F-FPOE. For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.</p>	disable

Variable	Description	Default
poe-status {enable   disable}	Enable Power over Ethernet. This option is only available with the FortiSwitch-324B-POE.	enable
priority-based-flow-control {enable   disable}	Enable priority-based flow control to avoid frame loss by stopping incoming traffic when a queue is congested. When priority-based flow control is disabled, 802.3 flow control can be used.	disable
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
security-mode {none   macsec}	Select no security or MACsec-based port security authentication. You cannot mix MACsec with ISL authentication.	none
speed <speed_str>	Set the speed of this port. Values depend on the switch model and port. For example: <ul style="list-style-type: none"> <li>1000auto—Autonegotiation (1 Gbps full-duplex only).</li> <li>100full—100 Mbps full-duplex.</li> <li>100half—100 Mbps half-duplex.</li> <li>10full—10 Mbps full-duplex.</li> <li>10half—10 Mbps half-duplex.</li> <li>auto—Auto-negotiation.</li> <li>10000cr—10 Gbps copper interface.</li> <li>10000full—10 Gbps full-duplex.</li> <li>10000sr—10 Gbps SFI interface.</li> <li>100full—1 Gbps full-duplex.</li> <li>25000cr—25 Gbps copper interface.</li> <li>25000full—25 Gbps full-duplex.</li> <li>25000sr—25 Gbps SFI interface.</li> <li>40000auto—Autonegotiation of the 40G-CR4 interface of FS-1048E.</li> <li>detect-by-module—Maximum speed supported by module.</li> </ul>	auto
status {down   up}	Set the administrative status of this interface: up or down.	up
storm-control-mode {disabled   global   override}	By default, you configure storm control on a system-wide level. Set this option to override if you want to configure storm control on a per-port level using the <code>config storm-control</code> command, which is only available when the <code>storm-control-mode</code> is set to <code>override</code> . Set this option to <code>disabled</code> to deactivate port-level storm-control configuration.	global
<b>config storm-control</b>		
broadcast {enable   disable}	Enable or disable storm control for broadcast traffic.	disable

Variable	Description	Default
burst-size-level <0-4>	Set the burst-size level for storm control. Use a higher number to handle bursty traffic. The maximum number of packets or bytes allowed for each burst-size level depends on the switch model. <b>NOTE:</b> This command is not available for the FS-108E, FS-108E-POE, FS-108-FPOE, FS-124E, FS-124E-POE, and FS-124E-FPOE models.	0
rate [0   2-10000000]	Specify the rate as packets-per-second. If you set the rate to zero, the system drops all packets (for the enabled traffic types).	500
unknown-multicast {enable   disable}	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

In the following example, port4 is configured:

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

## config switch prp channel

Use this command to configure a Parallel Redundancy Protocol (PRP) channel.

### Syntax

```
config switch prp channel
  edit {1 | 2}
    set status {enable | disable}
    set channel-port-pair <physical_port_pair>
    set vlan-id <1-4094>
    set vlan-id-cos <0-7>
    set vlan-id-tagged {enable | disable}
    set prp-internal-vlan <2-4094>
  next
end
```

Variable	Description	Default
status {enable   disable}	Enable or disable this PRP channel.	disable

Variable	Description	Default
channel-port-pair <physical_port_pair>	Select which port A and port B pair to use for this PRP channel. Enter <code>set channel-port-pair ?</code> to see the available physical port pairs.	No default
vlan-id <1-4094>	Enter the VLAN identifier of the supervision frame. This option is available only when <code>vlan-id-tagged</code> is set to enable.	1
vlan-id-cos <0-7>	Enter the class of service (CoS) value to be set in the VLAN tag of the supervision frame. This option is available only when <code>vlan-id-tagged</code> is set to enable.	0
vlan-id-tagged {enable   disable}	Enable or disable supervision frame VLAN ID tagging.	disable
prp-internal-vlan <2-4094>	Assign all MAC addresses of this PRP channel to this internal VLAN ID. <b>NOTE:</b> If you are using an HSR ring and a PRP channel in your network, you need to change the default value so that each HSR ring and PRP channel is in a different internal VLAN.	No default

## Example

The following example configures a PRP channel using port5, port6, and VLAN 4092:

```
config switch prp channel
  edit 1
    set status enable
    set channel-port-pair port5-port6
    set prp-internal-vlan 4092
  next
end
```

## config switch prp settings

Use this command to to configure PRP settings.

### Syntax

```
config switch prp settings
  set mac-da <0-255>
  set life-check-interval <2-60 seconds>
end
```

Variable	Description	Default
mac-da <0-255>	Specify the last 8 bits of the PRP supervision frame MAC DA.	0
life-check-interval <2-60 seconds>	Specify how often (in seconds) the PRP supervision frame is generated for each MAC address in the VDAN table.	2

## Example

The following example configures PRP settings:

```
config switch prp settings
  set mac-da 100
  set life-check-interval 30
end
```

## config switch ptp settings

Use this command to configure the Precision Time Protocol (PTP) global settings.

### Syntax

```
config switch ptp settings
  set status {enable | disable}
  set profile {default | name_of_PTP_profile}
end
```

Parameter	Description	Default value
status	Enable or disable PTP.	disable
profile	The default profile is automatically selected. <b>NOTE:</b> On some legacy platforms, the default profile must be manually selected.	default

## Example

The following example enables PTP and selects the newprofile PTP profile:

```
config switch ptp settings
  set status enable
  set profile newprofile
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. For an example, see [Appendix: FortiSwitch QoS template on page 510](#).

**NOTE:** You can configure only one dot1p map per switch on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.

### Syntax

```
config switch qos dot1p-map
  edit <dot1p map name>
    set description <text>
    set [priority-0|priority-1|priority-2|...priority-7] <queue number>
    set egress-pri-tagging {disable | enable}
  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
egress-pri-tagging {disable   enable}	Enable or disable priority tagging on outgoing frames. <b>NOTE:</b> This command is not available on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.	disable

### 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
    set egress-pri-tagging enable
  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. For an example, see [Appendix: FortiSwitch QoS template on page 510](#).

**NOTE:** You can configure only one DSCP map per switch on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.

### Syntax

```
config switch qos ip-dscp-map
  edit <ip-dscp map name>
    set description <text>
    config map
      edit <entry-name>
        set dffserv [ [ 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. For an example, see [Appendix: FortiSwitch QoS template on page 510](#).

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 rate-by {kbps | percent}
    set schedule {strict | round-robin | weighted}
    config cos-queue
      edit [queue-0 ... queue-7]
        set description <text>
        set drop-policy {taildrop | weighted-random-early-detection}
        set ecn {enable | disable}
        set max-rate <rate kbps>
        set min-rate <rate kbps>
        set max-rate-percent <percentage>
        set min-rate-percent <percentage>
        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
rate-by {kbps   percent}	Set whether the CoS queue rate is measured in kbps or by percentage.	kbps
schedule {strict   round-robin   weighted}	<p>Set the CoS queue scheduling.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ul>	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
drop-policy {taildrop   weighted-random-early-detection}	<p>Set the CoS queue drop policy.</p> <ul style="list-style-type: none"> <li>taildrop—When the queue is full, new packets are dropped.</li> <li>weighted-random-early-detection—When the queue reaches the packet-dropping threshold, packets start getting dropped randomly based on the probability defined in the <code>wred-slope</code> setting.</li> </ul> <p><b>NOTE:</b> For the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models, set the CoS queue drop policy under the <code>config switch global</code> command.</p>	taildrop
set ecn {enable   disable}	If you select random early detection in the CLI, you can enable explicit congestion notification (ECN) marking to indicate that congestion is occurring without just dropping packets. If you disable this option, the normal queue drop policy applies.	disable
max-rate <rate kbps>	If you set the rate-by to kbps, enter the maximum rate in kbps. Set the value to 0 to disable.	0

Variable	Description	Default
	<b>NOTE:</b> For the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models, the switch rounds the <code>max-rate</code> value to the nearest multiple of 16 internally. If the rounding result is 0, <code>max-rate</code> is disabled internally.	
<code>min-rate &lt;rate kbps&gt;</code>	If you set the <code>rate-by</code> to <code>kbps</code> , enter the minimum rate in kbps. Set the value to 0 to disable. <b>NOTE:</b> This command is not available on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.	0
<code>max-rate-percent &lt;percentage&gt;</code>	If you set the <code>rate-by</code> to <code>percent</code> , enter the maximum rate as a percentage of the link speed.	0
<code>min-rate-percent &lt;percentage&gt;</code>	If you set the <code>rate-by</code> to <code>percent</code> , enter the minimum rate as a percentage of the link speed. <b>NOTE:</b> This command is not available on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.	0
<code>weight &lt;value&gt;</code>	Enter the weight of weighted round robin scheduling. (applicable if the policy schedule is weighted )	1
<code>wred-slope &lt;value&gt;</code>	Enter the slope of WRED drop probability. <b>NOTE:</b> For the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models, set the QoS RED/WRED drop probability under the <code>config switch global</code> command.	45

## Example

The following example defines a QoS policy for queue 0:

```
config switch qos qos-policy
  edit policy1
    set rate-by kbps
    set schedule weighted
    config cos-queue
      edit queue-0
        set description "QoS policy for queue 0"
        set drop-policy weighted-random-early-detection
        set max-rate 20
        set min-rate 10
        set weight 5
        set wred-slope 15
      end
    end
  end
```

## config switch quarantine

**NOTE:** This command is available only in FortiLink mode.

Use this command to specify which MAC addresses to quarantine on the FortiSwitch unit.

### Syntax

```
config switch quarantine
  edit <MAC_address_to_quarantine>
    set cos-queue <0-7>
    set description <string>
    set drop {enable | disable}
    set policer <integer>
  end
```

Variable	Description	Default
<MAC_address_to_quarantine>	Enter the MAC address to quarantine.	No default
cos-queue <0-7>	Set the class-of-service queue for the quarantined device traffic. Use the <code>unset cos-queue</code> command to disable this setting.	No default
description <string>	Enter an optional description of the quarantined MAC address.	No default
drop {enable   disable}	Enable or disable whether quarantined device traffic is dropped.	disable
policer <integer>	Set the ACL policer for the quarantined device traffic.	0

## config switch raguard-policy

Use this command to specify the criteria that router advertisement (RA) messages must match before the RA messages are forwarded. If the RA messages match the criteria in the RA-guard policy, they are forwarded. If the RA messages do not match the criteria in the RA-guard policy, they are dropped.

IPv6 RA guard is supported on 2xx models and higher.

### Syntax

```
config switch raguard-policy
  edit <RA-guard policy name>
    set device-role {host | router}
    set managed-flag {Off | On}
    set other-flag {Off | On}
    set max-hop-limit <0-255>
    set min-hop-limit <0-255>
    set max-router-preference {high | medium | low}
    set match-src-addr <name_of_IPv6_access_list>
    set match-prefix <name_of_IPv6_prefix_list>
  next
end
```

Variable	Description	Default
<RA-guard policy name>	Enter the name of the RA-guard policy.	No default
device-role {host   router}	Set whether this policy applies to hosts or routers. If this option is set to <code>host</code> , all RA messages are dropped. If this option is set to <code>router</code> , the policy checks the other specified criteria.	host
managed-flag {Off   On}	Set to <code>On</code> for the policy to accept RA messages that are flagged with the M (managed address configuration) flag; if the RA messages are not flagged, they are dropped. Set to <code>Off</code> for the policy to accept RA messages that are <i>not</i> flagged with the M flag; if the RA messages are flagged, they are dropped. If this option is not set, the policy skips this check.	No default
other-flag {Off   On}	Set to <code>On</code> for the policy to accept RA messages that are flagged with the O (other configuration) flag; if the RA messages are not flagged, they are dropped. Set to <code>Off</code> for the policy to accept RA messages that are <i>not</i> flagged with the O flag; if the RA messages are flagged, they are dropped. If this option is not set, the policy skips this check.	No default
max-hop-limit <0-255>	Enter the maximum hop number for the policy to accept RA messages with a hop number equal or less than this value. If this option is not set, the policy skips this check.	0
min-hop-limit <0-255>	Enter the minimum hop number for the policy to accept RA messages with a hop number equal or more than this value. If this option is not set, the policy skips this check.	0
max-router-preference {high   medium   low}	Set the default router preference for the policy to accept RA messages with the router preference equal or less than this setting. When the router preference of RA messages is not set as high, medium, or low, RA guard acts as if the router preference was set to medium. If this option is not set, the policy skips this check.	No default
match-src-addr <name_of_IPv6_access_list>	Enter the name of the IPv6 access list for the policy to check if the source IPv6 address of the RA message matches an allowed address. The IPv6 access list must be created (with the <code>config router access-list6</code> command) before it is used in a policy.	No default
match-prefix <name_of_IPv6_prefix_list>	Enter the name of the IPv6 prefix list for the policy to check if the IPv6 address prefix of the RA message matches an allowed prefix. The IPv6 prefix list must be created (with the <code>config router prefix-list6</code> command) before it is used in a policy.	No default

## Example

The following example creates an IPv6 RA-guard policy:

```
config switch raguard-policy
  edit RApolicy1
    set device-role router
    set managed-flag On
    set other-flag On
    set max-hop-limit 100
    set min-hop-limit 5
    set max-router-preference medium
    set match-src-addr accesslist1
    set match-prefix prefixlist1
  next
end
```

## config switch security-feature

Use this command to configure security checks for incoming TCP/UDP packets. The packet is dropped if it matches one of the security rules that have been enabled.

### Syntax (for models FS-108D-POE, FS-112D-POE, FS-224D-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}
  set allow-mcast-sa {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 the 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 flags set.	disable
tcp_flag_SF	TCP packet with SYN and FIN flags set.	disable
tcp_flag_SR	TCP packet with SYN and RST flags 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
allow-mcast-sa	Ethernet packet whose source MAC address is multicast.	disable

## Syntax (for FS-1xxE, FS-1xxF, and FS-110G-FPOE)

```

config switch security-feature
  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 arp-mac-mismatch {enable | disable}
  set macsa-eq-macda {enable | disable}
  set sip-eq-dip {enable | disable}
  set tcp-port-eq {enable | disable}
  set udp-port-eq {enable | disable}
  set ip-pod {enable | disable}
  set icmp-frag {enable | disable}
  set tcp-frag-off-min {enable | disable}
  set tcp-syn-sp-less-1024 {enable | disable}
  set invalid-ipv4-hdr-len {enable | disable}
  set gratuitous-arp {enable | disable}
end

```

Variable	Description	Default
tcp-flag-zero	TCP packet with all flags set to zero.	disable
tcp-flag-FUP	TCP packet with FIN, URG, and PSH flags set.	disable
tcp-flag-SF	TCP packet with SYN and FIN flags set.	disable
tcp-flag-SR	TCP packet with SYN and RST flags set.	disable
arp-mac-mismatch	ARP packet with MAC source address mismatch between the MAC header and the ARP packet payload.	disable
macsa-eq-macda	Packet with source MAC address equal to the destination MAC address.	disable
sip-eq-dip	TCP packet with source IP address equal to the destination IP address.	disable
tcp-port-eq	TCP packet with the same source and destination TCP port.	disable
udp-port-eq	IP packet with the same source and destination UDP port.	disable
ip-pod	The IPv4/IPv6 packet length is larger than 64 kB.	disable
icmp-frag	Fragmented ICMP packet.	disable
tcp-frag-off-min	TCP non-initial fragments carry the TCP header.	disable
tcp-syn-sp-less-1024	TCP SYN packet with a source port less than 1024.	disable
invalid-ipv4-hdr-len	IPv4 packet with a header length greater than the total length. <b>NOTE:</b> This command is available only on the FS-124F, FS-124F-FPOE, FS-124F-POE, FS-148F, FS-148F-FPOE, and FS-148F-POE models.	disable

Variable	Description	Default
gratuitous-arp	Gratuitous ARP packet. <b>NOTE:</b> This command available only on the FS-108E, FS-108E-FPOE, FS-108E-POE, FS-108F, FS-108F-FPOE, FS-108F-POE, FS-124E, FS-124E-FPOE, FS-124E-POE, FS-148E, and FS-148E-POE models.	disable

## Syntax (for all other FortiSwitch 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 the same source IP address and destination IP address.	disable
tcp-flag	DoS attack checking for TCP flags.	disable
tcp-port-eq	TCP packet with the same source and destination TCP port.	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 flags set.	disable
v4-first-frag	DoS attack checking for IPv4 first fragment.	disable
udp-port-eq	IP packet with the same source and destination UDP port.	disable
tcp-hdr-partial	TCP packet with partial header.	disable
macsa-eq-macda	Packet with the same source MAC address and destination MAC address.	disable
allow-mcast-sa	Ethernet packet whose source MAC address is multicast.	disable
allow-sa-mac-all-zero	Ethernet packet whose source MAC address is all zeros.	disable

## Example

The following example configures various 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 action {allow | drop}
    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
action {allow   drop}	Select whether packets with the specified source static MAC address are allowed or dropped.	allow
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) address or a static address.	static
vlan-id <1-4095>	Enter the VLAN identifier.	1

### Example

```

config switch static-mac
  edit 1
    set action drop
    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 burst-size-level <0-4>
    set rate [0 | 2-10000000]
    set unknown-multicast {enable | disable}
    set unknown-unicast {enable | disable}
end

```

Variable	Description	Default
broadcast {enable   disable}	Enable or disable storm control for broadcast traffic.	disable
burst-size-level <0-4>	Set the burst-size level for storm control. Use a higher number to handle bursty traffic. The maximum number of packets or bytes allowed for each burst-size level depends on the switch model.	0
rate [0   2-10000000]	Specify the rate as packets-per-second. If you set the rate to zero, the system drops all packets (for the enabled traffic types).	500
unknown-multicast {enable   disable}	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 burst-size-level 2
    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
  end
end

```

Variable	Description	Default
<instance_id>	Enter an instance identifier. The range differs for the various FortiSwitch models.	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
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
<b>config stp-port</b>		
<port name>	Enter the name of the port.	No default
cost <cost_int>	Enter the cost of using this interface. Use <code>set cost ?</code> for suggested cost values based on link speed.	0
priority <priority_int>	Enter the priority of this interface. Use <code>set priority ?</code> 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 flood {enable | disable}
  set forward-time <fseconds_int>
  set hello-time <hseconds_int>
  set max-age <age>
  set max-hops <hops_int>
  set mclag-stp-bpdu {both | single}
  set name <name_str>
  set revision <rev_int>
  set status {enable | disable}
end
```

Variable	Description	Default
flood {enable   disable}	Set to <code>enable</code> if you want the STP packets arriving at any port to pass through the switch without being processed. Set to <code>disable</code> if you want to block STP packets arriving at any port. This command is available only when status is set to <code>disable</code> .	disable
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
mclag-stp-bpdu {both   single}	Set to <code>both</code> to allow both core switches of an MCLAG to transmit STP BPDUs. Set to <code>single</code> to prevent both core switches of an MCLAG from transmitting STP BPDUs.	both
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 aggregator-mode {bandwidth | count}
    set auto-isl <integer>
    set bundle [enable|disable]
      set min_bundle <integer>
      set max_bundle <integer>
    set description <description_str>
    set fortilink <integer>
    set isl-fortilink <integer>
    set lacp-speed {slow | fast}
    set mclag {disable | enable}
    set mclag-icl {disable | enable}
    set member-withdrawal-behavior {block | forward}
    set members <intf1 ... intfN>
    set mode {fortinet-trunk | lacp-active | lacp-passive | static}
    set fallback-port <port_name>
    set port-selection-criteria {src-ip | src-mac | dst-ip | dst-mac | src-dst-ip | src-dst-mac}
    set static-isl {enable | disable}
    set static-isl-auto-vlan {enable | disable}
  end
```

Variable	Description	Default
<trunk name>	Enter a name for the trunk.	No default
aggregator-mode {bandwidth   count}	Select how an aggregator groups ports when the trunk is in LACP mode. Select bandwidth to group ports into the aggregator with the largest bandwidth. Select count to group ports into the aggregator with the most ports.	bandwidth
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
fortilink <integer>	Set the FortiLink trunk.	0
isl-fortilink <integer>	Set the ISL FortiLink trunk.	0

Variable	Description	Default
lacp-speed {slow   fast}	Select fast to send an LACP message every second. Select slow to send an LACP message every 30 seconds.	slow
mclag {disable   enable}	Enable or disable multichassis LAG (MCLAG).	disable
mclag-icl {disable   enable}	Enable or disable the MCLAG inter-chassis link (ICL).	disable
member-withdrawal-behavior {block   forward}	Select how the port behaves after it withdraws because of loss-of-control packets.	block
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: <ul style="list-style-type: none"> <li>fortinet-trunk—use heartbeat packets to detect whether trunk members are available.</li> <li>lacp-active—use active LACP 802.3ad aggregation</li> <li>lacp-passive—use passive LACP 802.3ad aggregation</li> <li>static—use static aggregation, ignoring and not sending control messages</li> </ul>	static
fallback-port <port_name>	Select which port will stay up in LACP fallback mode so that a device not running LACP can still connect to the network.	No default
port-selection-criteria {src-ip   src-mac   dst-ip   dst-mac   src-dst-ip   src-dst-mac}	Select the port selection criteria: <ul style="list-style-type: none"> <li>src-ip—source IP address</li> <li>src-mac—source MAC address</li> <li>dst-ip—destination IP address</li> <li>dst-mac—destination MAC address</li> <li>src-dst-ip—both source and destination IP addresses</li> <li>src-dst-mac—both source and destination MAC addresses</li> </ul>	src-dst-ip
static-isl {enable   disable}	Available only in FortiLink mode. Enable to manually create an inter-switch link (ISL) trunk.	default
static-isl-auto-vlan {enable   disable}	Available only in FortiLink mode. Enable or disable automatic VLAN configuration on the ISL.	default

## 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: <ul style="list-style-type: none"> <li>src-ip – source IP address</li> <li>src-mac – source MAC address</li> <li>dst-ip – destination IP address</li> <li>dst-mac – destination MAC address</li> <li>src-dst-ip – both source and destination IP addresses</li> <li>src-dst-mac – both source and destination MAC addresses</li> </ul>	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-port

Use this command to configure DHCP snooping on VXLAN virtual ports. Virtual ports are configured automatically by the system; users cannot create them.

### Syntax

```

config switch virtual-port
  edit <virtual_port_name>
    set description <string>
    set dhcp-snooping {trusted | untrusted}
    set dhcp-snoop-learning-limit-check {enable | disable}
    set dhcp-snoop-learning-limit <1-16000>
  next
end

```

Variable	Description	Default
<virtual_port_name>	Enter a name for the virtual port. The name must be in the following format: vni.<VNI>.<remote_end_VTEP_IP_address> For example, if the VXLAN network identifier (VNI) is 100 and the remote end of the VXLAN tunnel is at 1.1.1.1, the virtual port name is vni.100.1.1.1.1.	No default
description <string>	Enter a description for the virtual port.	No default
dhcp-snooping {trusted   untrusted}	Set the interface to trusted or untrusted.	trusted
dhcp-snoop-learning-limit-check {enable   disable}	Enable or disable whether there is a limit for how many IP addresses are in the DHCP-snooping binding database for this virtual port. The set dhcp-snoop-learning-limit-check command is available only when dhcp-snooping has been set to untrusted.	disable
dhcp-snoop-learning-limit <1-16000>	Set the maximum number of IP addresses learned on this virtual port for the DHCP-snooping binding database. The set dhcp-snoop-learning-limit command is available only when dhcp-snoop-learning-limit-check is enabled.	5

### Example

The following example enables DHCP snooping on VNI 100 with the remote end of the VXLAN tunnel at 1.1.1.1. The number of IP addresses learned for the DHCP-snooping binding database has been limited to 100.

```

config switch virtual-port

```

```

edit vni.100.1.1.1.1
  set description "virtual port for VNI 100"
  set dhcp-snooping untrusted
  set dhcp-snoop-learning-limit-check enable
  set dhcp-snoop-learning-limit 100
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>
  next
end

```

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
  next
end

```

## config switch vlan

Use this command to configure VLANs.

## Syntax

```

config switch vlan
  edit <VLAN_ID>
    set access-vlan {enable | disable}
    set assignment-priority <1-255>
    set cos-queue <0-7>
    set description <description_str>
    set dhcp-snooping {enable | disable | monitor}
    set dhcp-snooping-verify-mac {enable | disable}
    set dhcp-snooping-option82 {enable | disable}
    set arp-inspection {enable | disable | monitor}
    set dhcp6-snooping {enable | disable}
    set igmp-snooping {enable | disable}
    set igmp-snooping-querier {enable | disable}
    set igmp-snooping-querier-addr <IPv4_address>
    set igmp-snooping-querier-version {2|3}
    set igmp-snooping-fast-leave {enable | disable}
    set igmp-snooping-proxy {enable | disable}
    set lan-segment {enable | disable}
    set lan-subvlans <VLAN_identifiers>
    set lan-internal-vlan <VLAN_identifier>
    set learning {enable | disable}
    set learning-limit <integer>
    set mld-snooping {enable | disable}
      set mld-snooping-fast-leave {enable | disable}
      set mld-snooping-querier {enable | disable}
      set mld-snooping-querier-addr <IPv6_address>
      set mld-snooping-proxy {enable | disable}
    set policer <integer>
    set private-vlan {enable | disable}
      set isolated-vlan <integer>
      set community-vlans <vlan_map>
    set rspan-mode {enable | disable}
    config dhcp-snooping-static-client
      set mac-addr <MAC_address>
      set switch-interface <interface_name>
      set ip-addr <IPv4_address>
    config igmp-snooping-static-group
      edit <group_name>
        set mcast-addr <IPv4_address>
        set members <interface_name1> <interface_name2>...
        set ignore-reports {enable | disable}
      end
    config mld-snooping-static-group
      edit <group_name>
        set mcast-addr <IPv6_address>
        set members <interface_name1> <interface_name2>...
        set ignore-reports {enable | disable}
      end
    config member-by-mac
    config member-by-ipv4
    config member-by-ipv6
    config member-by-proto
    config dhcp-server-access-list
  end

```

Variable	Description	Default
<vlan id>	Enter a VLAN identifier.	No default
access-vlan {enable   disable}	Set to <code>enable</code> to block FortiSwitch port-to-port traffic on this VLAN while allowing traffic to and from the FortiGate unit. Set to <code>disable</code> to allow normal VLAN traffic.	disable
assignment-priority <1-255>	Assign a priority to the VLAN. If there is more than one VLAN with the same name (specified in the <code>set description</code> command), FortiSwitchOS selects the VLAN with the lowest <code>assignment-priority</code> value (which is the highest priority) of the VLANs with names (specified in the <code>set description</code> command) that match the RADIUS Egress-VLAN-Name attribute.	128
cos-queue <0-7>	Specify which class of service (CoS) queue is used for traffic on this VLAN or use the <code>unset cos-queue</code> command to disable this setting. This command is available only in FortiLink mode.	No default
description <description_str>	Optionally, enter a description. If the Tunnel-Private-Group-Id attribute on the RADIUS server was set to the VLAN name, set the description to the same string. For example: <code>set description "newvlan"</code>	No default
dhcp-snooping {enable   disable   monitor}	Select the setting for IPv4 DHCP snooping: <ul style="list-style-type: none"> <li><code>enable</code>—Enable IPv4 DHCP snooping on this VLAN.</li> <li><code>disable</code>—Disable IPv4 DHCP snooping on this VLAN.</li> <li><code>monitor</code>—Monitor IPv4 DHCP snooping on this VLAN.</li> </ul>	disable
dhcp-snooping-verify-mac {enable   disable}	Enable or disable whether to verify the source MAC address. This option is available only if <code>dhcp-snooping</code> is set to <code>enable</code> .	disable
dhcp-snooping-option82 {enable   disable}	Enable or disable whether to insert option-82 fields. This option is available only if <code>dhcp-snooping</code> is set to <code>enable</code> .	disable
arp-inspection {enable   disable   monitor}	Specify one of the following: <ul style="list-style-type: none"> <li><code>enable</code>—Enable dynamic ARP inspection.</li> <li><code>disable</code>—Disable dynamic ARP inspection.</li> <li><code>monitor</code>—Monitor ARP packets.</li> </ul> <p><b>NOTE:</b> You must set <code>dhcp-snooping</code> to <code>enable</code> to be able to set <code>arp-inspection</code> to <code>enable</code> or <code>monitor</code>.</p>	disable
dhcp6-snooping {enable   disable}	Enable or disable IPv6 DHCP snooping for this VLAN.	disable

Variable	Description	Default
igmp-snooping {enable   disable}	Enable or disable IGMP snooping on the VLAN.	disable
igmp-snooping-fast-leave {enable   disable}	Enable or disable IGMP-snooping fast leave on this VLAN. This field is only available if igmp-snooping is enabled.	enable
igmp-snooping-querier {enable   disable}	Enable or disable whether periodic IGMP-snooping queries are sent to get IGMP reports. This field is only available if igmp-snooping is enabled.	disable
igmp-snooping-querier-addr <IPv4_address>	Required. Enter the IPv4 address for the IGMP-snooping querier. This field is only available if igmp-snooping-querier is enabled.	0.0.0.0
igmp-snooping-querier-version {2 3}	Select whether to use the IGMP-snooping querier version 2 or version 3.	2
igmp-snooping proxy {enable   disable}	Enable or disable the IGMP-snooping proxy on this VLAN. When the IGMP-snooping proxy is enabled, this VLAN sends IGMP reports. This field is only available if igmp-snooping is enabled.	disable
lan-segment {enable   disable}	Enable or disable the use of LAN segments.	disable
lan-subvlans <VLAN_identifiers>	Enter the VLAN identifiers to assign to the LAN segment. You can enter single VLANs or ranges of VLANs, separated by commas without white space. For example: "1,2-4,5,7,9-100". The value must be less than 4,096 characters. This field is only available if lan-segment is enabled.	No default
lan-internal-vlan <VLAN_identifier>	For the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models only.  After you enable LAN segments, FortiSwitchOS automatically assigns a VLAN for internal use. This VLAN cannot be used for any other purpose. If you want to assign a different internal VLAN, type set lan-internal-vlan ? to see a range of VLANs; however, these VLANs might not be available. If no VLANs are available to be used as an internal VLAN, the LAN segment configuration returns an error message.  This field is only available if lan-segment is enabled.	0
learning {enable   disable}	Enable or disable layer-2 learning on this VLAN.	enable
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

Variable	Description	Default
mld-snooping {enable   disable}	Enable or disable Multicast Listener Discovery (MLD) snooping for the this VLAN.	disable
mld-snooping-fast-leave {enable   disable}	Enable or disable MLD-snooping fast leave on this VLAN. This field is only available if mld-snooping is enabled.	enable
mld-snooping-querier {enable   disable}	Enable or disable whether periodic MLD-snooping queries are sent to get MLD reports. This field is only available if mld-snooping is enabled.	disable
mld-snooping-querier-addr <IPv6_address>	Required. Enter the IPv6 address for the MLD-snooping querier. This field if only available if mld-snooping-querier is enabled.	::
mld-snooping-proxy {enable   disable}	Enable or disable the MLD-snooping proxy on this VLAN. When the MLD-snooping proxy is enabled, this VLAN sends MLD reports. This field is only available if mld-snooping is enabled.	disable
policer <integer>	Set the policer for the traffic on this VLAN. This command is available only in FortiLink mode.	0
private-vlan {enable   disable}	Set to enable if this is a private VLAN.	disable
isolated-vlan <integer>	(Valid if private VLAN is enabled) Enter the isolated VLAN.	0
community-vlans <vlan_map>	(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
rspan-mode {enable   disable}	Enable or disable port mirroring using the remote switch port analyzer (RSPAN) on this VLAN.	disable
<b>config dhcp-snooping-static-client</b>		
mac-addr <MAC_address>	Specify a MAC address to bind to an IP address for this VLAN. Use the form of xx:xx:xx:xx:xx:xx.	00:00:00:00:00:00
switch-interface <interface_name>	Specify the switch interface to associate with this DHCP-snooping static entry. To find out which switch interfaces are valid, type set switch-interface ?.	No default
ip-addr <IPv4_address>	Specify the IPv4 address to bind to a MAC address for this VLAN.	0.0.0.0
<b>config igmp-snooping-static-group</b>		
<group_name>	Enter the IGMP static group name.	No default

Variable	Description	Default
mcast-addr <IPv4_address>	Enter the IPv4 multicast address for the IGMP static group.	0.0.0.0
members <interface_name1> <interface_name2>...	Enter the interfaces that belong to the IGMP static group.	No default
ignore-reports {enable   disable}	Enable or disable whether IGMP snooping ignores dynamic joins from other ports.	disable
<b>config mld-snooping-static-group</b>		
<group_name>	Enter the MLD static group name.	No default
mcast-addr <IPv6_address>	Enter the IPv6 multicast address for the MLD static group.	No default
members <interface_name1> <interface_name2>...	Enter the interfaces that belong to the MLD static group.	No default
ignore-reports {enable   disable}	Enable or disable whether MLD snooping ignores dynamic joins from other ports.	disable

## 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
  end

```

Variable	Description	Default
<b>config member-by-mac</b>		
edit <id>	For a new entry, enter an unused ID.	No 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
<b>config member-by-ipv4</b>		
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
<b>config member-by-ipv6</b>		
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
<b>config member-by-proto</b>		
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-snooping querier:

```
config switch vlan
  edit 100
    set igmp-snooping enable
    set igmp-snooping-querier enable
    set igmp-snooping-querier-addr 1.2.3.4
    set igmp-snooping-querier-version 3
  next
end
```

## config dhcp-server-access-list

Use this command to create a list of DHCP servers that DHCP snooping will include in the allowed server list. This list is used only if the `set dhcp-server-access-list` command has been enabled; see [config system global on page 218](#).

```
config switch vlan
  edit <vlan id>
    set dhcp-snooping enable
    set dhcp6-snooping enable
    config dhcp-server-access-list
      edit <string>
        set server-ip <xxx.xxx.xxx.xxx>
        set server-ip6 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>
      next
    end
  next
end
```

Variable	Description	Default
edit <vlan id>	Enter a VLAN identifier.	No default
dhcp-snooping enable	Enable for IPv4 DHCP snooping. The config <code>dhcp-server-access-list</code> command is available only after DHCP snooping (IPv4 or IPv6) has been enabled for that VLAN.	disable
dhcp6-snooping enable	Enable for IPv6 DHCP snooping. The config <code>dhcp-server-access-list</code> command is available only after DHCP snooping (IPv4 or IPv6) has been enabled for that VLAN.	disable
<b>config dhcp-server-access-list</b>		
edit <string>	Enter name of DHCP server access list	No default
server-ip <xxx.xxx.xxx.xxx>	If you enabled IPv4 DHCP snooping, enter Class A, B, or C IPv4 address for the DHCP server.	0.0.0.0
server-ip6 <xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx>	If you enabled IPv6 DHCP snooping, enter the IPv6 address for the DHCP server.	No default

## Example

The following example configures IPv4 DHCP snooping to include the specified DHCP server in the allowed server list:

```
config switch vlan
  edit 100
    set dhcp-snooping enable
    config dhcp-server-access-list
      edit "DHCPserver1"
        set server-ip 128.8.0.0
      next
    end
  next
end
```

The following example configures IPv6 DHCP snooping to include the specified DHCP server in the allowed server list:

```
config switch vlan
  edit 100
    set dhcp6-snooping enable
    config dhcp-server-access-list
      edit "DHCPserver1"
        set server-ip6 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234
      next
    end
  next
end
```

## config switch vlan-tpid

Use this command to configure the VLAN TPID profile for VLAN stacking (QnQ). Each VLAN TPID profile contains one value for the EtherType field.

The FortiSwitch unit supports a maximum of four VLAN TPID profiles, including the default (0x8100). The default VLAN TPID profile (0x8100) cannot be deleted or changed.

To configure VLAN stacking and to select which VLAN TPID profile to use, see [config switch interface on page 116](#).

### Syntax

```
config switch vlan-tpid
  edit <VLAN_TPID_profile_name>
    set ether-type <0x0001-0xffff>
  next
end
```

Variable	Description	Default
<VLAN_TPID_profile_name>	Enter a name for the VLAN TPID profile name.	No default
ether-type <0x0001-0xffff>	Enter a hexadecimal value for the EtherType field.	0x8100

## config switch-controller global

Use this command to configure system-wide switch options in FortiLink mode.

### Syntax

```
config switch-controller global
  set ac-data-port <1024-49150>
  set ac-dhcp-option-code <integer>
  set ac-discovery-mc-addr <Class-D IPv4 address>
  set ac-discovery-type {broadcast | dhcp | multicast | static}
  set ac-port <1024-49150>
  set echo-interval <1-600>
  set location <string>
  set name <string>
  set max-discoveries <0-64>
  set max-retransmit <0-64>
  set mgmt-mode {capwap | https}
  set source-ip <IPv4_address>
  set source-ip6 <IPv6_address>
  config ac-list
    edit <id>
      set ipv4-address <IPv4_address>
    next
  end
end
```

Variable	Description	Default
ac-data-port <1024-49150>	Set the switch-controller control port. Valid values are 1024-49150.	15250
ac-dhcp-option-code <integer>	Set the DHCP option code for CAPUTP AC.	138
ac-discovery-mc-addr <Class-D IPv4 address>	Set the discovery multicast address.	224.0.1.140
ac-discovery-type {broadcast   dhcp   multicast   static}	Select the AC discovery type: broadcast discovery, DHCP discovery, multicast discovery, or static configuration.	broadcast
ac-port <1024-49150>	Set the switch-controller control port.	5246
echo-interval <1-600>	Set the number of seconds before SWTP sends an echo request after joining AC.	30
location <string>	Enter the location.	No default
name <string>	Enter a name for the configuration.	No default
max-discoveries <0-64>	Set the maximum number of discovery request messages for every round.	3
max-retransmit <0-64>	Set the maximum number of retransmissions for the tunnel packet.	6

Variable	Description	Default
mgmt-mode {capwap   https}	Select whether FortiLink uses the CAPWAP protocol or HTTPS to manage switches.	capwap
source-ip <IPv4_address>	Enter the source IPv4 address for the FortiSwitch unit to communicate with the FortiGate device.	0.0.0.0
source-ip6 <IPv6_address>	Enter the source IPv6 address for the FortiSwitch unit to communicate with the FortiGate device.	No default
ac-list	Create a list of IPv4 addresses for AC static discovery. This command is only available when the ac-discovery-type is set to static.	No default.
<id>	Enter a unique integer to create a new entry.	No default.
ipv4-address <IPv4_address>	Enter a Class A, B, or C IPv4 address in the following format: xxx.xxx.xxx.xxx	No default.

## Example

The following example configures static discovery to find the IP address of the FortiGate unit (switch controller) that manages the FortiSwitch unit:

```
config switch-controller global
  set ac-discovery-type static
  config ac-list
    edit 1
      set ipv4-address <IPv4_address>
    next
  end
end
```

## config system

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

- [config system accprofile](#) on page 185
- [config system admin](#) on page 187
- [config system alias command](#) on page 189
- [config system alias group](#) on page 194
- [config system arp-table](#) on page 195
- [config system automation-action](#) on page 195
- [config system automation-stitch](#) on page 198
- [config system automation-trigger](#) on page 199
- [config system bluetooth](#) on page 201
- [config system bug-report](#) on page 201
- [config system certificate ca](#) on page 202
- [config system certificate crl](#) on page 203

- [config system certificate local on page 204](#)
- [config system certificate oosp on page 205](#)
- [config system certificate remote on page 206](#)
- [config system console on page 206](#)
- [config system dhcp server on page 207](#)
- [config system dns on page 213](#)
- [config system flan-cloud on page 214](#)
- [config system flow-export on page 215](#)
- [config system global on page 218](#)
- [config system interface on page 225](#)
- [config system ipv6-neighbor-cache on page 238](#)
- [config system link-monitor on page 239](#)
- [config system location on page 240](#)
- [config system ntp on page 244](#)
- [config system password-policy on page 245](#)
- [config system ptp interface-policy on page 247](#)
- [config system ptp profile on page 247](#)
- [config system schedule group on page 250](#)
- [config system schedule onetime on page 251](#)
- [config system schedule recurring on page 251](#)
- [config system settings on page 252](#)
- [config system sflow on page 253](#)
- [config system sniffer-profile on page 254](#)
- [config system snmp community on page 255](#)
- [config system snmp sysinfo on page 257](#)
- [config system snmp user on page 259](#)
- [config system vxlan on page 261](#)
- [config system web on page 263](#)

## config system accprofile

Use this command to add access profiles 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 alias-commands {<command-name> | all}
    set exec-alias-grp {none | read | read-write}
    set loggrp {none | read | read-write}
    set mntgrp {none | read | read-write}
    set netgrp {none | read | read-write}
    set pktmongrp {none | read | read-write}
    set routegrp {none | read | read-write}
```

```

set swcoregrp {none | read | read-write}
set swmonguardgrp {none | read | read-write}
set sysgrp {none | read | read-write}
set utilgrp {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 permission for administrative access.	none
alias-commands {all   <list>}	Specify the aliases and alias groups to include in the access profile or specify all. The aliases and alias groups specified for this access profile control which commands an administrator can run using the <code>execute alias commands</code> . Use a space to separate multiple items.	none
exec-alias-grp {none   read   read-write}	Specify one of the following options: <ul style="list-style-type: none"> <li>Select <code>none</code> to prevent access to the <code>execute alias configure</code> commands.</li> <li>Select <code>read</code> to provide access to the <code>execute alias configure {get   show   show-full-configuration}</code> command.</li> <li>Select <code>read-write</code> to provide access to the <code>execute alias configure {get   show   show-full-configuration   set   unset}</code> and <code>execute alias script</code> commands.</li> </ul>	none
loggrp {none   read   read-write}	Set the permission for logging access.	none
mntgrp {none   read   read-write}	Set the permission for critical system maintenance access .	none
netgrp {none   read   read-write}	Set the permission for network access.	none
pktmongrp {none   read   read-write}	Set the access permission for packet and flow capture functionality.	none
routegrp {none   read   read-write}	Set the permission for routing access.	none
swcoregrp {none   read   read-write}	Set the permission for switch core access.	none
swmonguardgrp {none   read   read-write}	Set the access permission for switch monitor and guard features.	none
sysgrp {none   read   read-write}	Set the permission for system access.	none
utilgrp {none   read   read-write}	Set the permission for utilities access.	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.

### Syntax

```

config system admin
  edit <admin_name>
    set accprofile <profile-name>
    set accprofile-override {enable | disable}
    set allow-remove-admin-session {enable | disable}
    set comments <comments_string>
    set force-password-change {enable | disable}
    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 wildcard-fallback {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>
    next
  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

Variable	Description	Default
accprofile-override {enable   disable}	Enable or disable whether the remote authentication server can override the access profile.	disable
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
force-password-change{enable   disable}	Enable or disable whether the administrator is forced to change the password when logging in next.	disable
gui-detail-panel-location {bottom   hide   side}	Choose the position of the log detail window.	bottom
{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 unit. 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. If you want to include the “?” character as part of the password: 1. Press Ctrl+v. 2. Type the “?” character .	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

Variable	Description	Default
	Starting in FortiSwitchOS 7.4.0, you can add multiple administrators with wildcards in their names.	
wildcard-fallback {enable   disable}	Enable or disable attempting authentication against wildcard accounts if authenticating this account fails. This option is available only when remote-auth is enabled and when wildcard is disabled.	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
{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 alias command

Use this command to grant an administrator access to individual configuration attributes, table entries, or CLI commands. You can also use this command to create a script to run multiple commands. Scripts are a simpler way to manage a large number of commands.

**Notes:**

- Configuration-type aliases cannot create or delete table entries. For example, under the `config switch interface` command, you cannot create a new interface name with the `edit <interface_name>` command.
- The `super_admin` administrator profile has access to all command aliases.

**Syntax**

```

config system alias command
  edit <alias_name or script_name>
    set description <string>
    set type {configuration | script}
    set path <path>
    set attribute <attribute-name>
    set permission {read | read-write}
    set table-listing {allow | deny}
    set limit-shown-attributes {disable | enable}
    set read-only-attributes <attribute-name>
    set table-ids-allowed <table-ID-value>
    set command <string>
    set table-entry-create {allow | deny}
  config script-arguments
    edit <argument_ID>
      set type {integer | string | table-id}
      set name <string>
      set help <string>
      set optional {enable | disable}
      set range {enable | disable}
      set range-delay <0-172800>
      set allowed-values <string>
    next
  end
next
end

```

Variable	Description	Default
<alias_name or script_name>	If the type will be configuration, enter an alias name for the command in this configuration. If the type will be script, enter a script name.  The alias or script name cannot be all or match an alias group name.	No default
description <string>	If the type will be configuration, enter a description of the command or a help message. It can be up to 80-characters long. The description is displayed with the alias name when you enter <code>execute alias configure {get   show   show-full-configuration   set   unset} ?</code> .  If the type will be script, enter a description of the script. It can be up to 80-characters long. The description is displayed with the script name when you enter <code>execute alias script ?</code> .	No default

Variable	Description	Default
type {configuration   script}	<p>The configuration type provides configuration-specific functionality to control <code>get</code>, <code>show</code>, <code>show-full-configuration</code>, <code>set</code>, and <code>unset</code> commands. You can also use the configuration type to limit accessible table entries and limit displayed attributes.</p> <p>The script type allows the administrator to create a list of CLI commands to run.</p>	configuration
path <path>	<p>Required. Enter the period-separated path to the CLI command.</p> <p>For example, enter <code>set path switch.lldp.profile</code> to apply the configuration to the <code>config switch lldp profile</code> command. Enter <code>set path system.interface</code> to apply the configuration to the <code>config system interface</code> command. You can specify only top-level objects, such as <code>system.interface</code>, <code>router.bgp</code>, or <code>system.snmp.settings</code>. If you specify child objects or child tables (such as <code>system.interface.ipv6</code>, <code>router.bgp.neighbor</code>, or <code>switch.lldp.profile.custom-tlv</code>), FortiSwitch returns an error.</p>	No default
attribute <attribute-name>	<p>Required. Enter the attribute that can be retrieved or modified. Enter <code>set attribute ?</code> to see the list of valid attributes. If you enter an invalid value, FortiSwitchOS returns an error.</p> <p>This option is available only when path has been set.</p>	No default
permission {read   read-write}	<p>Select <code>read</code> to allow this alias to be used by the <code>execute alias configure {get   show   show-full-configuration}</code> command. Select <code>read-write</code> to allow this alias to be used by the <code>execute alias configure {get   show   show-full-configuration   set   unset}</code> command.</p>	read
table-listing {allow   deny}	<p>Allow or prevent the listing of all entries by the <code>execute alias configure {get   show   show-full-configuration}</code> command commands.</p> <ul style="list-style-type: none"> <li>Select <code>allow</code> to permit all entries to be listed.</li> <li>Select <code>deny</code> to prevent the entries from being listed except for the entries specified in the <code>table-ids-allowed</code> setting. If <code>table-ids-allowed</code> is empty, a valid entry must be provided for listing.</li> </ul> <p>This option is available only when path has been set.</p>	deny
limit-shown-attributes {disable   enable}	<p>Enable or disable whether to limit the attributes displayed with the <code>show</code> and <code>get</code> commands. Selecting <code>disable</code> displays all attributes for the <code>show</code> and <code>get</code> commands. Selecting <code>enable</code> displays only the attributes listed in <code>attributes</code> and <code>read-only-attributes</code>.</p>	enable

Variable	Description	Default
read-only-attributes <attribute-name>	When <code>limit-shown-attributes</code> is enabled, you can enter additional attributes to display with the <code>show</code> and <code>get</code> commands. When you enter <code>read-only-attributes ?</code> to see a list of valid attributes, more attributes are available than when you enter <code>set attribute ?</code> . Read-only attributes can include child tables, child objects, and get-only attributes. You can list up to 31 attributes.	No default
table-ids-allowed <table-ID-value>	Specify which entries can be accepted by the <code>execute alias configure {get   show   show-full-configuration   set   unset}</code> command.  Enter <code>set table-ids-allowed ?</code> to see a list of valid entries. You can specify entries that do not currently exist; they can be created later.  If <code>table-listing</code> is set to <code>deny</code> , the <code>table-ids-allowed</code> entries are displayed when the user runs the <code>execute alias configure {get   show   show-full-configuration}</code> command without specifying any entry.  This option is available only when <code>path</code> has been set.	No default
command <string>	Enter the script command (within quotation marks) to be run. You can use the Enter key to separate command lines. Enter <code>set command ?</code> for formatting details.  This option is available only when <code>type</code> has been set to <code>script</code> .	No default
table-entry-create {allow   deny}	Allow or deny the creation of new table (or sub-table) entries.  This option is available only when <code>type</code> has been set to <code>script</code> . When <code>type</code> has been set to <code>configuration</code> , you cannot create any new table entries.	deny
<b>config script-arguments</b>		
<argument_ID>	Enter an identifier for the argument. The identifier must match the identifier used in the script.	No default
type {integer   string   table-id}	Enter the data type that the argument accepts.	string
name <string>	Enter the display name for the argument. You can use uppercase and lowercase letters, numbers, and hyphens. The display name is shown when the user runs the <code>execute alias script</code> command.	No default
help <string>	Enter a help message for the argument. You can use uppercase and lowercase letters, numbers, slashes, parentheses, brackets, commas, underscores, and hyphens. The help message is displayed when the user runs the <code>execute alias script</code> command.	No default

Variable	Description	Default
optional {enable   disable}	Enable this option to allow the user to omit entering a value for this argument. Disable this option to force the user to specify a value for this argument.	disable
range {enable   disable}	Enable this option to allow a range of integers, a range of table identifiers, or a comma-separated list of strings. Disable this option to allow only a single value for this argument.	disable
range-delay <0-172800>	Enter the number of seconds to delay between values when executing. This option is available only when range has been set to enable.	0
allowed-values <string>	Enter the values allowed for this argument. <ul style="list-style-type: none"> <li>If type is set to string, separate values with a space. For example: set allowed-values port1 port3 port7</li> <li>If type is set to integer, you can use ranges and comma-separated values, such as "1-10" or "1-10,3,11,55".</li> <li>If type is set to table-id and the table identifiers are integers, you can use both ranges and comma-separated values, such as "1-10" or "1-10,3,11,55".</li> </ul>	No default

## Examples

The following example creates two aliases for the config switch physical-port command.

- The port-description alias allows an administrator to change the set description value; when running a get or show command, the administrator will see only the description configuration.
- The port-status alias allows an administrator to change the set status value; the administrator will see both the description and port status configuration when running get or show commands.

```
config system alias command
edit "port-status"
    set description "View or change the port status."
    set type configuration
    set path "switch.physical-port"
    set attribute "status"
    set permission read-write
    set limit-shown-attributes enable
    set read-only-attributes "description"
next
edit "port-description"
    set description "View or change the port description."
    set type configuration
    set path "switch.physical-port"
    set attribute "description"
    set permission read-write
    set limit-shown-attributes enable
next
end
```

The following example creates two scripts. Both scripts list the switch mac-address table.

- The `mac-list` script is more flexible because it requires that the user specify the VLANs to list the MAC addresses from.
- The `list-mac-by-port-and-vlan-customer-AAA` script is more controlled because it allows the user to see the MAC addresses learned on the specified VLANs.

```

config system alias command
  edit "list-mac-by-port-and-vlan-customer-AAA"
    set description "List MAC addresses on your VLANs and ports."
    set type script
    set command "diag switch mac-address filter clear
diag switch mac-address filter port-id-map 3-8
diag switch mac-address filter vlan-map 1000-1010
diag switch mac-address list
diag switch mac-address filter clear"
  next
  edit "mac-list"
    set description "List MAC addresses learned on the provided VLANs"
    set type script
    set command "diag switch mac-address filter clear
diag switch mac-address filter vlan-map $1
diag switch mac-address list | grep -i mac
diag switch mac-address filter clear"
    config script-arguments
      edit 1
        set name "VLAN-ID-map"
        set help "List of VLANs to check"
      next
    end
  next
end
end

```

## config system alias group

Use this command to specify alias groups to bundle different alias commands together for easy assignment.

### Syntax

```

config system alias group
  edit <alias_group_name>
    set description <string>
    set commands <alias_command_list>
  end

```

Variable	Description	Default
<alias_group_name>	Enter a name for the alias group. The name cannot be all or match an alias name.	No default
description <string>	Enter a description of the command alias group. It can be up to 80-characters long.	No default
commands <alias_command_name>	Enter a list of command aliases. Use a space to separate them.	No default

## Example

This example shows how to create a group of two command aliases:

```
config system alias group
  edit aliasgroup1
    set description "Alias group for config switch physical-port."
    set commands port-status port-description
  end
```

## config system arp-table

Use this command to manually add ARP table entries to the FortiSwitch unit. 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 automation-action

Use this command to configure the action that is performed when the trigger of an automation stitch occurs.

## Syntax

```

config system automation-action
  edit <name>
    set action-type {alert | cli-script | email | snmp-trap | webhook}
    set accprofile <string>
    set email-body <string>
    set email-from <string>
    set email-subject <string>
    set email-to <email_address>
    set headers <string>
    set http-body <string>
    set method {delete | get | patch | post | put}
    set minimum-interval <0-2592000>
    set port <1-65535>
    set protocol {http | https}
    set script <string>
    set snmp-trap {fsStitchTrap1 | fsStitchTrap2 | fsStitchTrap3 | fsStitchTrap4 | fsStitchTrap5}
    set uri <string>
  next
end

```

Variable	Description	Default
<name>	Name of the action configuration.	No default
action-type {alert   cli-script   email   snmp-trap   webhook}	Select the type of action to perform: <ul style="list-style-type: none"> <li>alert—Display an alert in the console.</li> <li>cli-script—Run a CLI script.</li> <li>email—Send a notification email.</li> <li>snmp-trap—Generate an SNMP trap.</li> <li>webhook—Send data to a uniform resource identifier (URI), such as an IP address or URL.</li> </ul>	alert
accprofile <string>	Specify the access profile required to run the CLI script. This option is available only when action-type is set to cli-script.	No default
email-body <string>	Enter the body of the email. By default, the log message is sent. This option is available only when action-type is set to email.	%%log%%
email-from <string>	Enter the name of the sender of the email. This option is available only when action-type is set to email.	No default
email-subject <string>	Enter the subject of the email. This option is available only when action-type is set to email.	No default
email-to <email_address>	Enter the email address or addresses that the email will be sent to when automation stitch is triggered.	none

Variable	Description	Default
	This option is available only when <code>action-type</code> is set to <code>email</code> .	
<code>headers &lt;string&gt;</code>	Enter the request headers. This option is available only when <code>action-type</code> is set to <code>webhook</code> .	none
<code>http-body &lt;string&gt;</code>	If necessary, enter the request body. Use a serialized JSON string. This option is available only when <code>action-type</code> is set to <code>webhook</code> .	No default
<code>method {delete   get   patch   post   put}</code>	Select the request method: DELETE, GET, PATCH, POST, or PUT. This option is available only when <code>action-type</code> is set to <code>webhook</code> .	post
<code>minimum-interval &lt;0-2592000&gt;</code>	Select how many seconds must pass before the action can be performed again.	0
<code>port &lt;1-65535&gt;</code>	Enter the port number that this protocol will use. If the protocol is set to <code>http</code> , the default port is 80. If the protocol is set to <code>https</code> , the default port is 443. This option is available only when <code>action-type</code> is set to <code>webhook</code> .	80
<code>protocol {http   https}</code>	Enter the request protocol, either HTTP or HTTPS. This option is available only when <code>action-type</code> is set to <code>webhook</code> .	http
<code>script &lt;string&gt;</code>	Specify the name and path to the CLI script. This option is available only when <code>action-type</code> is set to <code>cli-script</code> .	No default
<code>snmp-trap {fsStitchTrap1   fsStitchTrap2   fsStitchTrap3   fsStitchTrap4   fsStitchTrap5}</code>	Select which SNMP trap is generated: <ul style="list-style-type: none"> <li><code>fsStitchTrap1</code>—This custom SNMP trap can be triggered from automation stitch.</li> <li><code>fsStitchTrap2</code>—This custom SNMP trap can be triggered from automation stitch.</li> <li><code>fsStitchTrap3</code>—This custom SNMP trap can be triggered from automation stitch.</li> <li><code>fsStitchTrap4</code>—This custom SNMP trap can be triggered from automation stitch.</li> <li><code>fsStitchTrap5</code>—This custom SNMP trap can be triggered from automation stitch.</li> </ul> This option is available only when <code>action-type</code> is set to <code>snmp-trap</code> .	No default

Variable	Description	Default
uri <string>	Required. Enter the uniform resource identifier (URI), such as an IP address or URL.  This option is available only when action-type is set to webhook.	No default

## Example

This example shows how to display an alert in the console when the automation stitch is triggered:

```
config system automation-action
  edit testaction
    set action-type alert
    set minimum-interval 1200
  next
end
```

## config system automation-stitch

Use this command to specify the trigger and action for an automation stitch.

### Syntax

```
config system automation-stitch
  edit <name>
    set status {enable | disable}
    set trigger <trigger_name>
    set action <action_name>
  next
end
```

Variable	Description	Default
<name>	Name of the automation-stitch configuration.	No default
status {enable   disable}	Enable or disable this automation stitch.	enable
trigger <trigger_name>	Enter the name of the trigger for this automation stitch.	No default
action <action_name>	Enter the name of the action configuration for this automation stitch.	none

## Example

This example shows how to specify the trigger, action, and status for an automation stitch:

```
config system automation-stitch
  edit teststitch
    set status enable
    set trigger testtrigger
    set action testaction
  next
```

```
end
```

## config system automation-trigger

Use this command to specify the trigger for an automation stitch. The trigger causes an action to be performed.

### Syntax

```
config system automation-trigger
  edit <trigger_name>
    set trigger-type {event-based | scheduled}
    set event-type {config-change | event-log | reboot}
    set logid <log_ID>
    set trigger-frequency {daily | hourly | monthly | weekly}
    set trigger-hour <0-23>
    set trigger-minute <0-59>
    set trigger-day <1-31>
    set trigger-weekday <friday | monday | saturday | sunday | thursday | tuesday | wednesday>
  config fields
    edit <entry_ID>
      set name <string>
      set value <string>
    next
  end
next
end
```

Variable	Description	Default
<trigger_name>	Name of the trigger configuration.	No default
trigger-type	Select the type of trigger: <ul style="list-style-type: none"> <li>event-based—Event-based trigger.</li> <li>scheduled—Scheduled trigger.</li> </ul>	event-based
event-type	Select the type of event to trigger the automation-stitch action: <ul style="list-style-type: none"> <li>config-change—Configuration change.</li> <li>event-log—Use the log ID as the trigger.</li> <li>reboot—After the switch restarts, the action is triggered.</li> </ul> This option is available only when the trigger-type is set to event-based.	config-change
logid <log_ID>	Enter the log ID to trigger the action. The range of values is 1-65535. If you use the full 10-digit entry, the first four digits are truncated. <p>This option is available only when the trigger-type is set to event-based and event-type is set to event-log.</p>	0
trigger-frequency {daily   hourly   monthly   weekly}	Select whether the automation-stitch action is performed on a daily, hourly, monthly, or weekly basis.	daily

Variable	Description	Default
	This option is available only when the <code>trigger-type</code> is set to <code>scheduled</code> .	
<code>trigger-hour &lt;0-23&gt;</code>	Select which hour of the day the automation-stitch action is performed. This option is available only when the <code>trigger-type</code> is set to <code>scheduled</code> and the <code>trigger-frequency</code> is set to <code>daily</code> or <code>monthly</code> , or <code>weekly</code> .	0
<code>trigger-minute &lt;0-59&gt;</code>	Select which minute of the hour the automation-stitch action is performed. This option is available only when the <code>trigger-type</code> is set to <code>scheduled</code> .	0
<code>trigger-day &lt;1-31&gt;</code>	Select which day of the month the automation-stitch action is performed. This option is available only when the <code>trigger-type</code> is set to <code>scheduled</code> and the <code>trigger-frequency</code> is set to <code>monthly</code> .	1
<code>trigger-weekday &lt;friday   monday   saturday   sunday   thursday   tuesday   wednesday&gt;</code>	Select which day of the week the automation-stitch action is performed. This option is available only when the <code>trigger-type</code> is set to <code>scheduled</code> and the <code>trigger-frequency</code> is set to <code>weekly</code> .	No default
<b>config fields</b>	This option is available only when the <code>event-type</code> is <code>event-log</code> and the <code>logid</code> is set. Starting in FortiSwitchOS 7.2.2, you can configure multiple fields for the automation trigger. The action is only performed if all conditions are valid (using AND logic).	
<code>&lt;entry_ID&gt;</code>	Enter an identifier for this entry.	No default
<code>name &lt;string&gt;</code>	Enter a name for this field.	No default
<code>value &lt;string&gt;</code>	Enter a value for this field. <ul style="list-style-type: none"> <li>Use an asterisk to match any character string of any length, including 0-characters long. For example, use <code>set value "*1567*"</code> to match values of 81567 and 156789.</li> <li>Use square brackets to match one of the multiple characters. For example, use <code>set value "[aA]dmin"</code> to match values of <code>admin</code> and <code>Admin</code>.</li> </ul>	No default

## Example

This example shows how to generate a log entry when port1 is down:

```
config system automation-trigger
  edit "port1Down"
    set event-type event-log
    set logid 100001401
    config fields
      edit 1
```

```

        set name "switch.physical-port"
        set value "port1"
    next
end
next
end

```

This example shows how to configure the action to be triggered on an hourly basis, 30 minutes into the hour:

```

config system automation-trigger
edit testtrigger
    set trigger-type scheduled
    set trigger-frequency hourly
    set trigger-minute 30
next
end

```

## config system bluetooth

Use this command to configure Bluetooth.

### Syntax

```

config system bluetooth
    set pin <string>
    set status {disable | enable}
end

```

Variable	Description	Default
pin <string>	Enter the Bluetooth pair personal identification number (PIN).	1234
status {disable   enable}	Enable or disable support for Bluetooth.	disable

## 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/WtE48FeMA0GCSqGSIb3DQEBCwUAMGgxZARBgoJ
> kiaJk/IsZAEZFgNvcmcxFzAVBgoJkiaJk/IsZAEZFgdjaWxvZ29uMQswCQYDVQGG
> EwJVUzEQMA4GA1UEChMHQ01Mb2dvbjEzMBCGA1UEAxMQQ01Mb2dvbiBPU0cgQ0Eg
> MTAeFw0xNDA0MzAxNDE4MDhaFw0zNDA0MzAxNDE4MDhaMGgxZARBgoJkiaJk/Is
> ZAEZFgNvcmcxFzAVBgoJkiaJk/IsZAEZFgdjaWxvZ29uMQswCQYDVQGGewJVUzEQ
> MA4GA1UEChMHQ01Mb2dvbjEzMBCGA1UEAxMQQ01Mb2dvbiBPU0cgQ0EgMTCCASIw
> DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMQzSb9Uc37VuIyt5XxcYYkc6K
> XpYihHgsKTQp6YYB4XHVimouHafMYoFsnenrcgf2NGFDvi919x9mnL77920JqGr
> LijieMiFEyP1nhGW8C6nJjkSsXLbgZNh9u6U+0oAbspsFRwdHDZ0I7gIHSJ2zuiY
> CkMAVjw9TN44Q4IFCvSI7mfzZgBH7AW1sbgznqAJswQhQGTPxZAxubItesyduD
> vj8tz9eb5u8J03iQ/LYhMspNnxcPTFdaLn2v82NAFTtCrZdCd7aLj1DM0DPEX7Nw
> V/rt/1+t1scg1YyEoUnlPYuSQN0Q6Aj5i1GcKpvnFS00y91GY11T1vZJ4F0CAwEA
> AaN+MHwwDwYDVR0TAQH/BAUwAwEB/zAObgNVHQ8BAF8EBAMCAQYwHQYDVR0OBBYE
> FP7bnvI4TIqtrM+KGgCvedJiQpuHMB8GA1UdIwQYMBaAFP7bnvI4TIqtrM+KGgCv
> FP7bnvI4TIqtrM+KGgCvedJiQpuHMB8GA1UdIwQYMBaAFP7bnvI4TIqtrM+KGgCv
> edJiQpuHMBkGA1UdEQSMBCBDMNhQGNpbG9nb24ub3JnMA0GCSqGSIb3DQEBCwUA
> A4IBAQCq5KUHQNg51uh1pxKMXQ98ADj2bNzQbswdAFs1Pow8tTZIBMwhdrq02ZHC
> XPyp2IHxfv+G+pMV1JFtdR0fy8ivi1Mnyj0bEGh1Ss3kvvU7d1z3XwPxpNcwDqs
> 1K6RRg4zpnWCFPCliAkPDsDban1B6A6zJXqOpGgzwoU3dZbPe5sYLgkWZ02/8MI
> eAEk7zoU1ZPSZiu5HghPafKuE1HYshvsak090tRgC6VLvaSLonZlwr0GuFVGdewH
> 4jR1HpENH7QiLCBINGCoJgDi3qiFosw3M2+0ExevE1afj2Usm4oZir+Uty0rvR8D
> 03RHH8yYbZ9rw0kuwTkJE03bYDXH
> -----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/HQXRH41mBwGmjKdBSHUBVUZTka2FtD1oLMWE2mTq1c9GMUz0DokPfoqxkjkjma5mWv4/w
A5XdQ001QmTeMZK/X5OSFmSS
set private-key "-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIBnjbABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5/vf1VQB/28CAggA
MBQGCCqGSib3DQMHBAgZorM0z1nPNASCAViZk4wTZYMP10e7NwyxqvLND3LxUaV
UG1XpUSPfnUP4YgrV2d0Uijc1j5M7MS341cMVKZ7G1pS/6jvxUr0NamQv4j7JsJ0
t3G7LMkzcTiep26GUCy55Qt+iob7lh0iiKa+4uPOq/Mzy+84AwnRNLfIhevHPsYb
rk4UbwNOFb0ZD9i06+UrFLsRgntp/v1DyBgAoBojKxB/4j0G299QamnzPz4qneBc
HtPqTMPELyqtT6w4cmnwp6Ti200Ar9c44mKdyyAVZKie+Iu/4pSVBNSfuC+jjtmC
k8OrCrG14NwrhbTY9zEnGxBRR1NMTEBBTqAQNYWtjUEQVjmY1GAJA3/oBQe7l8C/
G/IUVvc/aaqMvsKSNfDpgZaudTDe1Wxi1792ADGh7zs1ls+ykH9nmqh7BPfm30Nv
f801hXgq01Lvo4v1xdC0w5oAeCyG1bTY5ZnXJFm0HCp0kA==
-----END ENCRYPTED PRIVATE KEY-----
"

set csr "-----BEGIN CERTIFICATE REQUEST-----
MIIBNzCB4gIBADBqMQswCQYDVQQIEwJjYTESMBAQA1UEBxMjc3Vubn12YWx1MREw
DwYDVQQKEWhmb3J0aw5ldENMAAsGA1UECzMEZmFkYzEQMA4GA1UEAxMHZXhhbXBs
ZTETMBEGCSqGSib3DQEJARYEcm9vdDBcMA0GCSqGSib3DQEBAQUAA0sAMEgCQQDK
XH/MC1KtKkZJiQDFb6IXHLYsSVbJzF0K30s3CVmKZvJQSBnmV8aq3fJjN281rrFT
iUovVdBzwCF5jKbxsrPLAGmBAAGgEzARBgNVHRMxChMIQ0E6RkFMU0UwDQYJKoZI
hvcNAQEFBQADQQB96NU+Xjds83/6VRSzsyxeVxAGVD7F9Npuji8r/MpxPiMT0PQM
G8Wg//26ZqpWjuPq2V1+7QU4MDk3B5VUJSEF
-----END CERTIFICATE REQUEST-----
"
```

## config system certificate ocsps

Use this command to configure the OCSF server certificate.

### Syntax

```
config system certificate ocsps
  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 OCSF check or revoke the certificate if the server is unavailable.	revoke
url <string>	Enter the URL for the OCSF server.	No default

## Example

This example shows how to configure the OCSP server certificate:

```
config system certificate ocs
  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 configure the FortiSwitchOS console.

### Syntax

```
config system console
  set baudrate <speed>
  set hostname-display-length <4-35>
  set login {enable | disable}
  set mode {batch | line}
  set output {standard | more}
end
```

Variable	Description	Default
baudrate <speed>	Set the console port baud rate. Select one of 9600, 19200, 38400, 57600, or 115200.	115200
hostname-display-length <4-35>	Set the maximum number of characters shown for the host name in the CLI prompt.	17
login {enable   disable}	Enable or disable whether users can log in with the FortiSwitchOS console port.	enable

Variable	Description	Default
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.	standard

## Example

This example shows how to configure the console:

```
config system console
  set hostname-display-length 30
  set baudrate 57600
  set login enable
  set mode batch
  set output standard
end
```

## config system dhcp server

Use this command to configure DHCP servers.

### Syntax

```
config system dhcp server
  edit <id>
    set auto-configuration {enable | disable}
    set conflicted-ip-timeout <integer>
    set default-gateway <xxx.xxx.xxx.xxx>
    set dns-server1 <xxx.xxx.xxx.xxx>
    set dns-server2 <xxx.xxx.xxx.xxx>
    set dns-server3 <xxx.xxx.xxx.xxx>
    set dns-service {default | local | specify}
    set domain <string>
    set filename <string>
    set interface <string>
    set lease-time <integer>
    set netmask <xxx.xxx.xxx.xxx>
    set next-server <xxx.xxx.xxx.xxx>
    set ntp-server1 <xxx.xxx.xxx.xxx>
    set ntp-server2 <xxx.xxx.xxx.xxx>
    set ntp-server3 <xxx.xxx.xxx.xxx>
    set ntp-service {default | local | specify}
    set status {enable | disable}
    set tftp-server <xxx.xxx.xxx.xxx>
    set timezone <00-75>
    set timezone-option {default | disable | specify}
    set vci-match {enable | disable}
    set vci-string <VCI_strings>
    set wifi-ac1 <xxx.xxx.xxx.xxx>
```

```

set wifi-ac2 <xxx.xxx.xxx.xxx>
set wifi-ac3 <xxx.xxx.xxx.xxx>
set wins-server1 <xxx.xxx.xxx.xxx>
set wins-server2 <xxx.xxx.xxx.xxx>
config exclude-range
  edit <id>
    set end-ip <xxx.xxx.xxx.xxx>
    set start-ip <xxx.xxx.xxx.xxx>
  next
end
config ip-range
  edit <id>
    set end-ip <xxx.xxx.xxx.xxx>
    set start-ip <xxx.xxx.xxx.xxx>
  next
end
config options
  edit <id>
    set code <integer>
    set ip <IP_addresses>
    set type {fqdn | hex | ip | string}
    set value <string>
  next
end
config reserved-address
  edit <id>
    set action {assign | block | reserved}
    set circuit-id {<string> | <hex>}
    set circuit-id-type {hex | string}
    set description <string>
    set ip <xxx.xxx.xxx.xxx>
    set mac <xx:xx:xx:xx:xx:xx>
    set remote-id {<string> | <hex>}
    set remote-id-type {hex | string}
    set type {mac | option82}
  next
end
next
end

```

Variable	Description	Default
<id>	Enter the identifier.	No default
auto-configuration {enable   disable}	Enable or disable automatic configuration. Auto configuration allows the DHCP server to dynamically assign IP addresses to hosts on the network connected to the interface	enable
conflicted-ip-timeout <integer>	Enter the number of seconds before a conflicted IP address is removed from the DHCP range and is available to be reused. The range is 60-8640000 seconds.	1800

Variable	Description	Default
default-gateway <xxx.xxx.xxx.xxx>	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.	0.0.0.0
dns-server1 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the DNS server 1. This option is only available when dns-service is set to specify.	0.0.0.0
dns-server2 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the DNS server 2. This option is only available when dns-service is set to specify.	0.0.0.0
dns-server3 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the DNS server 3. This option is only available when dns-service is set to specify.	0.0.0.0
dns-service {default   local   specify}	Select how DNS servers are assigned to DHCP clients. Select local to use the IP address of the DHCP server interface for the client's DNS server IP address. Select default for clients to be assigned the FortiSwitch unit's configured DNS servers. Select specify to enter the IPv4 address for up to three DNS servers.	specify
domain <string>	Enter the domain name suffix for the IP addresses that the DHCP server assigns to the clients.	No default
filename <string>	Enter the name of the boot file on the TFTP server.	No default
interface <string>	Enter the name of the interface. The DHCP server can assign IP configurations to clients connected to this interface.	No default
lease-time <integer>	The lease time determines the length of time an IP address remains assigned to a client. After the lease expires, the address is released for allocation to the next client that requests an IP address.  Enter the lease time in seconds. The range is 300-8640000. The default lease time is seven days.	604800
netmask <xxx.xxx.xxx.xxx>	Enter the netmask of the addresses that the DHCP server assigns.	0.0.0.0
next-server <xxx.xxx.xxx.xxx>	Enter the IPv4 address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.	0.0.0.0

Variable	Description	Default
ntp-server1 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the NTP server 1. This option is only available when ntp-service is set to specify.	0.0.0.0
ntp-server2 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the NTP server 2. This option is only available when ntp-service is set to specify.	0.0.0.0
ntp-server3 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the NTP server 3. This option is only available when ntp-service is set to specify.	0.0.0.0
ntp-service {default   local   specify}	Select how Network Time Protocol (NTP) servers are assigned to DHCP clients. Select local to use the IP address of the DHCP server interface for the client's NTP server IP address. Select default for clients to be assigned the FortiSwitch unit's configured NTP servers. Select specify to enter the IPv4 address for up to three NTP servers.	specify
status {enable   disable}	Enable or disable this DHCP configuration.	enable
tftp-server <string>	You can configure multiple Trivial File Transfer Protocol (TFTP) servers for a Dynamic Host Configuration Protocol (DHCP) server. For example, you may want to configure a main TFTP server and a backup TFTP server.  Enter the hostname or IP address of each TFTP server in quotes. Separate multiple server entries with spaces.	No default
timezone <00-75>	Enter the time zone to be assigned to DHCP clients. This option is only available if timezone-option is set to specify.	(GMT+12:00)Eniwetok,Kwajalein)
timezone-option {default   disable   specify}	Select how the DHCP server sets the client's time zone. Select disable for the DHCP server to not set the client's time zone. Select default for clients to be assigned the FortiSwitch unit's configured time zone. Select specify to enter the time zone to be assigned to DHCP clients.	disable
vci-match {enable   disable}	Enable or disable vendor class identifier (VCI) matching. When enabled, only DHCP requests with a matching VCI are served.	disable

Variable	Description	Default
vci-string <VCI_strings>	Enter one or more VCI strings. This option is only available if vci-match is set to enable.	No default
wifi-ac1 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the WiFi Access Controller 1 (DHCP option 138, RFC 5417).	0.0.0.0
wifi-ac2 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the WiFi Access Controller 2 (DHCP option 138, RFC 5417).	0.0.0.0
wifi-ac3 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the WiFi Access Controller 3 (DHCP option 138, RFC 5417).	0.0.0.0
wins-server1 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the WINS server 1.	0.0.0.0
wins-server2 <xxx.xxx.xxx.xxx>	Enter the IPv4 address for the WINS server 2.	0.0.0.0
<b>config exclude-range</b>		
<id>	Enter the identifier.	No default
end-ip <xxx.xxx.xxx.xxx>	Enter the end of the IP address range that will not be assigned to clients.	0.0.0.0
start-ip <xxx.xxx.xxx.xxx>	Enter the start of the IP address range that will not be assigned to clients.	0.0.0.0
<b>config ip-range</b>		
<id>	Enter the identifier.	No default
end-ip <xxx.xxx.xxx.xxx>	Enter the end of the DHCP IP address range.	0.0.0.0
start-ip <xxx.xxx.xxx.xxx>	Enter the start of the DHCP IP address range.	0.0.0.0
<b>config options</b>		
<id>	Enter the identifier.	No default
code <integer>	Select the DHCP option code. The range is 0-255.	9
ip <IP_addresses>	If type is set to ip, enter the IP addresses.	No default
type {fqdn   hex   ip   string}	Select the format of the DHCP option: fully qualified domain name, hexadecimal, IP address, or string.	hex
value <string>	Enter the DHCP option value. This option is available when type is set to fqdn, hex, or string.	No default

Variable	Description	Default
<b>config reserved-address</b>		
<id>	Enter the identifier.	No default
action {assign   block   reserved}	Select how the DHCP server configures the client with the reserved MAC address. Select assign for the DHCP server to configure the client with this MAC address like any other client. Select block to prevent the DHCP server from assigning IP settings to the client with this MAC address. Select reserved for the DHCP server to assign the reserved IP address to the client with this MAC address.	reserved
circuit-id {<string>   <hex>}	Enter the DHCP option-82 Circuit ID of the client that will get the reserved IP address. The circuit-id format is controlled by the circuit-id-type setting. This option is only available when type is set to option82.	No default
circuit-id-type {hex   string}	Select whether the format of circuit-id is hexadecimal or string. This option is only available when type is set to option82.	string
description <string>	Enter a description of this entry.	No default
ip <xxx.xxx.xxx.xxx>	Enter the IPv4 address to be reserved for the MAC address. This option is only available when action is set to reserved.	0.0.0.0
mac <xx:xx:xx:xx:xx:xx>.	Enter the MAC address of the client that will get the reserved IP address. This option is only available when type is set to mac.	00:00:00:00:00:00
remote-id {<string>   <hex>}	Enter the DHCP option-82 Remote ID of the client that will get the reserved IP address. This option is only available when type is set to option82.	No default
remote-id-type {hex   string}	Select whether the format of remote-id is hexadecimal or string. This option is only available when type is set to option82.	string
type {mac   option82}	Select whether to match the IP address with the MAC address or DHCP option 82.	mac

## Example

This example shows how to configure a DHCP server:

```
config system dhcp server
edit 1
```

```
set default-gateway 50.50.50.2
set domain "FortiswitchTest.com"
set filename "text1.conf"
set interface "svi10"
config ip-range
  edit 1
    set end-ip 50.50.0.10
    set start-ip 50.50.0.5
  next
end
set lease-time 360
set netmask 255.255.0.0
set next-server 60.60.60.2
config options
  edit 1
    set value "dddd"
  next
end
set tftp-server "1.2.3.4"
set timezone-option specify
set wifi-ac1 5.5.5.1
set wifi-ac2 5.5.5.2
set wifi-ac3 5.5.5.3
set wins-server1 6.6.6.1
set wins-server2 6.6.6.2
set dns-server1 7.7.7.1
set dns-server2 7.7.7.2
set dns-server3 7.7.7.3
set ntp-server1 8.8.8.1
set ntp-server2 8.8.8.2
set ntp-server3 8.8.8.3
next
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_ipv6>	Enter the secondary IPv6 DNS server IP address.	::
primary <dns_ipv4>	Enter the primary DNS server IP address.	0.0.0.0
secondary <dns_ipv4>	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 flan-cloud

Use this command to configure FortiLAN Cloud or FortiLink over HTTPS.

### Syntax

```
config system flan-cloud
  set interval <integer>
  set name <FortiLAN_Cloud_FQDN_IP_address | FortiLink_IPv4_address>
  set port <port_number>
  set service-type {flan-cloud | fortilink-https}
  set source-ip <IPv4_address>
  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.	3

Variable	Description	Default
name <FortiLAN_Cloud_FQDN_IP_address   FortiLink_IPv4_address>	If you are using FortiLAN Cloud, enter the fully qualified domain name or IP address for the FortiLAN Cloud. If you are using FortiLink with HTTPS, enter the FortiLink IPv4 address.	fortiswitch-dispatch.forticloud.com
port <port_number>	Port number used to connect to FortiLAN Cloud.	443
service-type {flan-cloud   fortilink-https}	If you are using FortiLAN Cloud, set service-type to flan-cloud. If you are using FortiLink with HTTPS, set service-type to fortilink-https.	flan-cloud
source-ip <IPv4_address>	Enter the source IPv4 address for the FortiSwitch unit to communicate with the FortiGate device.	0.0.0.0
status {enable   disable}	Select whether FortiLAN Cloud or FortiLink with HTTPS is active or inactive.	disable

## Example

This example shows how to configure FortiLAN Cloud:

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

## config system flow-export

You can sample IP packets on a FortiSwitch unit and then export the data in NetFlow format or Internet Protocol Flow Information Export (IPFIX) format.

The maximum number of concurrent flows is defined by the FortiSwitch model. When this limit is exceeded, the oldest flow expires and is exported.

### Syntax

```
config system flow-export
  set filter <string>
  set format {netflow1 | netflow5 | netflow9 | ipfix}
  set identity <hexadecimal>
  set level {ip | mac | port | proto | vlan}
  set max-export-pkt-size <integer>
  set template-export-period <1-60>
  set timeout-general <integer>
  set timeout-icmp <integer>
  set timeout-max <integer>
  set timeout-tcp <integer>
```

```

set timeout-tcp-fin <integer>
set timeout-tcp-rst <integer>
set timeout-udp <integer>
config collectors
  edit <collector_name>
    set ip <IPv4_address>
    set port <port_number>
    set transport {sctp | tcp | udp}
  end
config aggregates
  edit <aggregate_ID>
    set ip <IPv4_address_mask>
  end
end
end

```

Variable	Description	Default
filter <string>	Specify the Berkeley packet filter (BPF) to use. For example, set filter "host 33.33.33.2".	No default
format {netflow1   netflow5   netflow9   ipfix}	You can set the format of the exported flow data as NetFlow version 1, NetFlow version 5, NetFlow version 9, or IPFIX sampling. <b>NOTE:</b> When the export format is NetFlow version 5, the sample rate used in the exported packets is derived from the lowest port number where sampling is enabled. Fortinet recommends that administrators using NetFlow version 5 set the sample rate consistently across all ports.	netflow9
identity <hexadecimal>	Required. Enter a unique number to identify which FortiSwitch unit the data originates from. The range of values is 0x00000000-0xFFFFFFFF. If identity is not specified, the "Burn in MAC" value is used instead (see get system status).	0x00000000
level {ip   mac   port   proto   vlan}	You can set the flow-tracking level to one of the following: - ip—The FortiSwitch unit collects the source IP address and destination IP address from the sample packet. <ul style="list-style-type: none"> <li>• mac—The FortiSwitch unit collects the source MAC address and destination MAC address from the sample packet.</li> <li>• port—The FortiSwitch unit collects the source IP address, destination IP address, source port, destination port, and protocol from the sample packet.</li> <li>• proto—The FortiSwitch unit collects the source IP address, destination IP address, and protocol from the sample packet.</li> <li>• v1an—The FortiSwitch unit collects the source IP address, destination IP address, source port, destination port, protocol, and VLAN from the sample packet.</li> </ul>	ip
max-export-pkt-size <integer>	Set the maximum size in bytes of exported packets in the application level. The range of values is 512-9216.	512

Variable	Description	Default
template-export-period <1-60>	Set the number of minutes before the template is exported.	5
timeout-general <integer>	Set the general timeout in seconds for the flow session. The range of values is 60-604800.	3600
timeout-icmp <integer>	Set the ICMP timeout for the flow session. The range of values is 60-604800.	300
timeout-max <integer>	Set the maximum number of seconds before the flow session times out. The range of values is 60-604800.	604800
timeout-tcp <integer>	Set the TCP timeout for the flow session. The range of values is 60-604800.	3600
timeout-tcp-fin <integer>	Set the TCP FIN flag timeout for the flow session. The range of values is 60-604800.	300
timeout-tcp-rst <integer>	Set the TCP RST flag timeout for the flow session. The range of values is 60-604800.	120
timeout-udp <integer>	Set the UDP timeout for the flow session. The range of values is 60-604800.	300
<b>config collectors</b>		
<collector_name>	Enter the name of the flow-export collector.	No default
ip <IPv4_address>	Enter the IP address for the collector. The default is 0.0.0.0. Setting the value to "0.0.0.0" or "" disables this feature. The format is xxx.xxx.xxx.xxx.	0.0.0.0
port <port_number>	Enter the port number for the collector. The range of values is 0-65535. The default port for NetFlow is 2055; the default port for IPFIX is 4739.	0
transport {sctp   tcp   udp}	You can set exported packets to use UDP, TCP, or SCTP for transport.	udp
<b>config aggregates</b>		
<id>	Enter the identifier.	No default
<IPv4_address_mask>	Enter the IPv4 address and mask to match. All matching sessions are aggregated into the same flow.	No default

## Example

This example shows how to configure flow export:

```
config system flow-export
  set format ipfix
  set level ip
  config collectors
    edit flowone
      set ip 169.254.3.1
      set port 5
```

```

        set transport tcp
    next
end
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 {Fortinet_802.1x_CA | Fortinet_CA | Fortinet_CA2 | Fortinet_Sub_CA2 |
    Fortinet_fsw_cloud_CA}
  set 802.1x-certificate {Fortinet_802.1x | Fortinet_Factory | Fortinet_Factory2 | Fortinet_
    Firmware}
  set admin-concurrent {enable | disable}
  set admin-lockout-duration <time_int>
  set admin-lockout-threshold <failed_int>
  set admin-password-hash {pbkdf2 | pbkdf2-high | sha1 | sha256}
  set admin-restrict-local {enable | disable}
  set admin-scp {enable | disable}
  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 alertrd-relog {enable | disable}
  set alert-interval <1-1440 minutes>
  set allow-subnet-overlap {enable | disable}
  set arp-inspection-monitor-timeout <5-10080 minutes>
  set arp-timeout <seconds>
  set asset-tag <string>
  set cfg-save {automatic | manual | revert}
  set cfg-revert-timeout <10-2147483647>
  set clt-cert-req {enable | disable}
  set csr-ca-attribute {enable | disable}
  set daily-restart {enable | disable}
  set detect_ip_conflict {enable | disable}
  set dhcp-client-location {description | hostname | intfname | mode | vlan}
  set dhcp-option-format {ascii | legacy}
  set dhcp-remote-id {hostname | ip | mac}
  set dhcp-server-access-list {enable | disable}
  set dhcp-snoop-client-req {drop-untrusted | forward-untrusted}
  set dhcps-db-exp <number_of_seconds>
  set dhcps-db-per-port-learn-limit <number_of_entries>
  set dh-params {1024 | 1536 | 2048 | 3072 | 4096 | 6144 | 8192}
  set dst {enable | disable}
  set hostname <unithostname>
  set image-rotation {enable | disable}
  set ip-conflict-ignore-default {enable | disable}
  set ipv6-accept-dad <0 | 1 | 2>
  set ipv6-all-forwarding {enable | disable}
  set kernel-crashlog {enable | disable}
  set kernel-devicelog {enable | disable}

```

```

set l3-host-expiry {enable | disable}
set ldapconntimeout <ldaptimeout_msec>
set post-login-banner "<string>"
set pre-login-banner "<string>"
set private-data-encryption {enable | disable}
set radius-coa-port <port_number>
set radius-port <radius_port>
set remoteauthtimeout <timeout_sec>
set reset-button {enable | disable}
set revision-backup-on-logout {enable | disable}
set revision-backup-on-upgrade {enable | disable}
set single-psu-fault {enable | disable}
set strong-crypto {enable | disable}
set tcp-mss-min <48-10000>
set tcp6-mss-min<48-10000>
set timezone <timezone_number>

```

end

Variable	Description	Default
802.1x-ca-certificate {Fortinet_802.1x_CA   Fortinet_CA   Fortinet_CA2   Fortinet_Sub_CA2   Fortinet_fsw_cloud}	Set the CA certificate for port security (802.1x): <ul style="list-style-type: none"> <li>Fortinet_802.1x_CA—Select this CA if you are using 802.1x authentication.</li> <li>Fortinet_CA—Select this CA if you want to use the factory-installed certificate.</li> <li>Fortinet_CA2—Select this CA if you want to use the factory-installed certificate.</li> <li>Fortinet_Sub_CA2—Select this CA if you want to use the factory-installed certificate.</li> <li>Fortinet_fsw_ccloud—Select this CA if you are using FortiLAN Cloud.</li> </ul>	Fortinet_802.1x_CA
802.1x-certificate {Fortinet_802.1x   Fortinet_Factory   Fortinet_Factory2   Fortinet_Firmware}	Set the certificate for port security (802.1x): <ul style="list-style-type: none"> <li>Fortinet_802.1x—This certificate is embedded in the firmware and is the same on every unit (not unique). It has been signed by a public CA. This is the default certificate for 802.1x authentication.</li> <li>Fortinet_Factory—This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.</li> <li>Fortinet_Factory2—This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.</li> <li>Fortinet_Firmware—This certificate is embedded in the firmware and is the same on every unit (not unique). It has been signed by a proper CA. It is not recommended to use it for server-type functionality since any other unit could use this same certificate to spoof the identity of this unit.</li> </ul>	Fortinet_802.1x

Variable	Description	Default
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 <code>policy-auth-concurrent</code> for firewall authenticated users.	enable
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 <code>admin-lockout-threshold</code> to set the number of failed attempts that will trigger the lockout.	60
admin-lockout-threshold <failed_int>	Set the threshold, or number of failed attempts, before the account is locked out for the <code>admin-lockout-duration</code> .	3
admin-password-hash {pbkdf2   pbkdf2-high   sha1   sha256}	Select which hash algorithm is used to encode passwords for new administrator accounts: <ul style="list-style-type: none"> <li>• <code>pbkdf2</code>—Use the PBKDF2 hash algorithm with a lower iteration count.</li> <li>• <code>pbkdf2-high</code>—Use the PBKDF2 hash algorithm with a higher iteration count.</li> <li>• <code>sha1</code>—Use the SHA1 hash algorithm.</li> <li>• <code>sha256</code>—Use the SHA256 hash algorithm.</li> </ul>	sha256
admin-restrict-local {enable   disable}	Enable/disable local admin authentication restriction when remote authenticator is up and running. <ul style="list-style-type: none"> <li>• <code>enable</code>—Enable local admin authentication restriction.</li> <li>• <code>disable</code>—Disable local admin authentication restriction.</li> </ul>	disable
admin-scp {enable   disable}	Enable to allow system configuration download by the secure copy (SCP) protocol.	disable
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 <code>admintimeout</code> interval is 480 minutes (8 hours). To improve security, keep the idle timeout at the default value of 5 minutes.	5

Variable	Description	Default
alrtd-relog {enable   disable}	Enable or disable re-logs when a sensor exceeds its threshold.	disable
alert-interval	<b>NOTE:</b> This command is only available after the <code>alrtd-relog</code> option has been enabled. Set how often an alert is generated for temperature sensors when they exceed their set thresholds.	30
allow-subnet-overlap {enable   disable}	Use this command to allow two interfaces to include the same IP address in the same subnet. The command applies only between the mgmt interface and an internal interface. <b>Note:</b> Different interfaces cannot have overlapping IP addresses or subnets. <b>Caution: For advanced users only.</b> Use this only for existing network configurations that cannot be changed to eliminate IP address overlapping.	disable
arp-inspection-monitor-timeout <5-10080 minutes>	Set the number of minutes before the MAC addresses, VLAN identifiers, and IP addresses that were learned from ARP traffic are removed from the DHCP-snooping database. When <code>arp-inspection-monitor-timeout</code> is set to 0, the ARP traffic entries do not expire and are not removed from the DHCP-snooping database.	1440
arp-timeout <seconds>	Set the number of seconds before dynamic ARP entries are removed from the cache.	180
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
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: <ul style="list-style-type: none"> <li><code>automatic</code> automatically save the configuration after every change.</li> <li><code>manual</code> manually save the configuration using the <a href="#">execute acl key-compact on page 380</a> command.</li> <li><code>revert</code> manually save the current configuration and then revert to that saved configuration after <code>cfg-revert-timeout</code> expires.</li> </ul> Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode.	automatic
cfg-revert-timeout <10-2147483647>	After the configuration change, wait the specified number of seconds, restart the FortiSwitch unit, and revert to the last saved configuration if the configuration is not manually saved within the period.	600

Variable	Description	Default
	<p>Before FortiSwitchOS 7.2.1, there was no reboot before the configuration was reverted.</p> <p>This command is available only when <code>cfg-save</code> is set to <code>revert</code>.</p>	
<code>clt-cert-req {enable   disable}</code>	Enable or disable the requirement to have a client certificate to log in to the GUI.	disable
<code>csr-ca-attribute {enable   disable}</code>	Enable to use the CA attribute in your certificate. Some CA servers reject CSRs that have the CA attribute.	enable
<code>daily-restart {enable   disable}</code>	Enable to restart the FortiSwitch unit every day. The time of the restart is controlled by <code>restart-time</code> .	disable
<code>detect_ip_conflict {enable   disable}</code>	Enable the Detect IP Conflict feature.	enable
<code>dhcp-client-location {description   hostname   intfname   mode   vlan}</code>	<p>Select which parameters to include to describe the client location. Separate multiple parameters with a space.</p> <ul style="list-style-type: none"> <li><code>description</code>—Include the interface description.</li> <li><code>hostname</code>—Include the host name.</li> <li><code>intfname</code>—Include the interface name.</li> <li><code>mode</code>—Include the mode.</li> <li><code>vlan</code>—Include the VLAN.</li> </ul>	intfname vlan mode
<code>dhcp-option-format {ascii   legacy}</code>	<p>Select the format for the DHCP string:</p> <ul style="list-style-type: none"> <li><code>ascii</code>—This format allows the user to choose the values for the <code>circuit-id</code> and <code>remote-id</code> fields.</li> <li><code>legacy</code>—This format generates a predefined fixed format for the <code>circuit-id</code> and <code>remote-id</code> fields.</li> </ul>	ascii
<code>dhcp-remote-id {hostname   ip   mac}</code>	<p>Select which parameters to include in the <code>remote-id</code> field:</p> <ul style="list-style-type: none"> <li><code>hostname</code>—Include the host name.</li> <li><code>ip</code>—Include the IP address.</li> <li><code>mac</code>—Include the MAC address.</li> </ul>	mac
<code>dhcp-server-access-list {enable   disable}</code>	Set to <code>disable</code> for DHCP snooping to allow any DHCP server from trusted interfaces. Set to <code>enable</code> for DHCP snooping to allow only DHCP servers that are included in the allowed server list.	disable
<code>dhcp-snoop-client-req {drop-untrusted   forward-untrusted}</code>	<p>Select which transmission mode to use for broadcasting client DHCP packets:</p> <ul style="list-style-type: none"> <li><code>drop-untrusted</code>—Client packets are broadcasted on trusted ports in the VLAN.</li> <li><code>forward-untrusted</code>—By default, client packets are broadcasted on all ports in the VLAN.</li> </ul>	drop-untrusted

Variable	Description	Default
dhcps-db-exp <number_of_seconds>	Set the number of seconds for a DHCP-snooping server database entry to be kept. The range of values is 300-259200.	86400
dhcps-db-per-port-learn-limit <number_of_entries>	Set the maximum number of DHCP server entries that are learned per interface. The range of values is 0-1024.	64
dh-params {1024   1536   2048   3072   4096   6144   8192}	Specify the minimum size (in bits) of the Diffie-Hellman prime for SSH/HTTPS.	2048
dst {enable   disable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiSwitch unit adjusts the system time when the time zone changes to daylight saving time and back to standard time.	enable
hostname <unithostname>	Enter a name to identify this FortiSwitch unit. 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.	enable
ip-conflict-ignore-default {enable   disable}	Enable or disable IP conflict detection for the default IP address.	enable
ipv6-accept-dad <0   1   2>	Specify whether to accept IPv6 duplicate address detection (DAD). Set to 0 to disable DAD. Set to 1 to enable DAD. Set to 2 to enable DAD and disable IPv6 operation if a MAC-based duplicate link-local address is found.	1
ipv6-all-forwarding {enable   disable}	Enable or disable IPv6 forwarding.	enable
kernel-crashlog {enable   disable}	Enable or disable whether to log a kernel crash.	enable
kernel-devicelog {enable   disable}	Enable or disable the capture of kernel device messages to the log.	enable
l3-host-expiry {enable   disable}	Enable or disable layer-3 host expiry.	disable
ldapconntimeout <ldaptimeout_msec>	LDAP connection timeout in msec	500

Variable	Description	Default
post-login-banner "<string>"	Enter a message for the system post-login banner.	No default
pre-login-banner "<string>"	Enter a message for the system pre-login banner.	No default
private-data-encryption {enable   disable}	Enable or disable private data encryption using an AES 128-bit key.	disable
radius-coa-port <port_number>	Set the port number to be used for the RADIUS change of authorization (CoA).	3799
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
remoteauthtimeout <timeout_sec>	<p>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.</p> <p>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.</p>	5
reset-button {enable   disable}	<p>Enable or disable the FortiSwitch hardware Reset button:</p> <ul style="list-style-type: none"> <li>Set this option to <code>enable</code> to be able to use the FortiSwitch hardware Reset button, even if the OS is running.</li> <li>Set this option to <code>disable</code> to disable the FortiSwitch hardware Reset button while the OS is running.</li> </ul>	enable
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
single-psu-fault {enable   disable}	<p>Enable this option to have the ALARM LED turn red when only one power supply unit (PSU) is connected. If you disable this option, the ALARM LED will not turn red, even when one or two PSUs are connected.</p> <p><b>NOTE:</b> This option is only available for the FSR-112D-POE (system part number P17080-04 or later) and FSR-216F-POE models. You can check the system part number with the <code>get system status</code> command.</p>	disable

Variable	Description	Default
strong-crypto {enable   disable}	Strong encryption only allows strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by Firefox.	enable
tcp-mss-min <48-10000>	Enter the minimum allowed TCP MSS value in bytes.	48
tcp6-mss-min <48-10000>	Enter the minimum allowed TCP MSS value in bytes.	48
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

## Example

This example shows how to set your private data encryption key:

```
S548DN5018000535 # config system global
S548DN5018000535 (global) # set private-data-encryption enable
S548DN5018000535 (global) # end
Please type your private data encryption key (32 hexadecimal numbers):
0123456789abcdefabcdef0123456789
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0123456789abcdefabcdef0123456789
Your private data encryption key is accepted.
```

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 dhcp-vendor-specific-option <string>
set external {enable | disable}
set fail-detect {enable | disable}
  set fail-detect-option {link-down | detectserver}
  set fail-alert-method {link-down | link-failed-signal}
  set fail-alert-interfaces {port1 port2 ...}
set icmp-redirect {enable | disable}
set interface <interface_name>
set ip <interface_ipv4mask>
set log {enable | disable}
set l2-interface <interface_name>
set mode <static | dhcp>
  set dhcp-client-identifier <client_name_str>
  set distance <1-255>
  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 src-check {disable | loose | strict}
set src-check-allow-default {enable | disable}
set status {down | up}
set type {loopback | physical | vlan | vxlan}
set vlanid <id_number>
set vrf <string>
set vrrp-virtual-mac {enable | disable}
config ipv6
  set ip6-address <ipv6_netmask>
  set ip6-allowaccess <access_types>
  set autoconf {disable | enable}
  set ip6-unknown-mcast-to-cpu {disable | enable}
  set ip6-mode {dhcp | static}
  set ip6-dns-server-override {disable | enable}
  set dhcp6-information-request {disable | enable}
  set ip6-send-adv {disable | enable}
  set ip6-manage-flag {disable | enable}
  set ip6-other-flag {disable | enable}
  set ip6-max-interval <4-1800>
  set ip6-min-interval <3-1350>
  set ip6-link-mtu <integer>
  set ip6-reachable-time <0-3600000>
  set ip6-retrans-time <0-2147483647>
  set ip6-default-life <0-9000>
  set ip6-hop-limit <0-255>
  set vrip6_link_local {enable | disable}
  set vrrp-virtual-mac6 {enable | disable}
config ip6-extra-address
  edit <prefix_ipv6>
```

```

    next
end
config vrrp6
    edit <virtual_router_identifier>
        set accept-mode {enable | disable}
        set adv-interval <1-255>
        set preempt {enable | disable}
        set priority <1-255>
        set start-time <1-255>
        set status {enable | disable}
        set vrdst6 <IPv6_address>
        set vrgrp <1-65535>
        set vrip6 <IPv6_address>
    next
end
config ip6-prefix-list
    edit <prefix_ipv6>
        set autonomous-flag {disable | enable}
        set onlink-flag {disable | enable}
        set preferred-life-time <0-2147483647>
        set valid-life-time <0-2147483647>
    end
end
config secondaryip
    edit <id>
        set ip <IP_address_and_netmask>
        set allowaccess <access_types>
config vrrp
    edit <VRID_int>
        set adv-interval <seconds_int>
        set backup-vmac-fwd {enable | disable}
        set netmask <xxx.xxx.xxx.xxx>
        set preempt {enable | disable}
        set priority <prio_int>
        set start-time <seconds_int>
        set status {enable | disable}
        set version {2 | 3}
        set vrdst <ipv4_addr>
        set vrgrp <integer>
        set vrip <ipv4_addr>
    next
end

```



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:	Varies for each interface.

Variable	Description	Default
	<p>http https ping radius-acct snmp ssh telnet.</p> <p>Separate each type with a space.</p> <p>To add or remove an option from the list, retype the complete list as required.</p>	
alias <name_string>	<p>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.</p> <p>This option is available only when the interface type is physical.</p>	No default.
bfd {enable   disable   global}	<p>The status of bidirectional forwarding detection (bfd) on this interface:</p> <ul style="list-style-type: none"> <li>• enable – enable BFD and ignore global BFD configuration.</li> <li>• disable – disable BFD on this interface.</li> <li>• global – use the BFD configuration in system settings for the virtual domain to which this interface belongs.</li> </ul>	global
bfd-desired-min-tx <interval_msec>	<p>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.</p>	50
bfd-detect-mult <multiplier>	<p>Select the BFD detection multiplier. This option is available only when bfd is enabled.</p>	3
bfd-required-min-rx <interval_msec>	<p>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.</p>	50
description <text>	<p>Optionally, enter up to 63 characters to describe this interface.</p>	No default
dhcp-relay-service {enable   disable}	<p>Enable to provide DHCP relay service on this interface. The DHCP type relayed depends on the setting of dhcp-relay-type.</p> <p>There must be no other DHCP server of the same type (regular or ipsec) configured on this interface.</p>	disable
dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}	<p>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.</p> <p>Do not set dhcp-relay-ip to 0.0.0.0. This option is available only when dhcp-relay-service is enabled.</p>	No default
dhcp-relay-option82 {enable   disable}	<p>Enable to allow option-82 insertion in the DHCP relay. This option is available only when dhcp-relay-service is enabled.</p>	disable

Variable	Description	Default
dhcp-vendor-specific-option <string>	Set the value for DHCP vendor-specific option 43.	No default
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
interface <interface_name>	Enter the name of the interface. This option is available only when vlanid is set.	internal
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
l2-interface <interface_name>	Enter the name of the layer-2 interface. This option is available only when the interface type is physical.	No default
mode <interface_mode>	Configure the connection mode for the interface as one of: <ul style="list-style-type: none"> <li>static—Configure a static IP address for the interface.</li> <li>dhcp—Configure the interface to receive its IP address from an external DHCP server.</li> </ul>	static

Variable	Description	Default
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
distance <1-255>	Enter the distance of learned routes. This command is available only when mode is set to dhcp.	5
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	
src-check {disable   loose   strict}	Set to <code>disable</code> if you do not want to use unicast reverse-path forwarding (uRPF). Set to <code>strict</code> to ensure that the packet was received on the same interface that the router uses to forward the return packet. Set to <code>loose</code> to ensure that the routing table includes the source IP address of the packet.	disable
src-check-allow-default {enable   disable}	If you disable the <code>src-default-route-check</code> option, the packet is dropped if the source IP address is not found in the routing table. If you enable the <code>src-default-route-check</code> option, the packet is allowed even if the source IP address is not found in the routing table, but the default route is found in the routing table. This option is available only when <code>src-check</code> is set to <code>loose</code> .	disable

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   physical   vlan   vxlan}	<p>Enter the type of interface. <b>NOTE:</b> Some types are read only and are set automatically by hardware.</p> <ul style="list-style-type: none"> <li>• <code>loopback</code>—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.</li> <li>• <code>physical</code>—a physical interface.</li> <li>• <code>vlan</code>—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.</li> <li>• <code>vxlan</code>— a virtual extensible LAN interface.</li> </ul>	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
vrf <string>	<p>Assign this virtual routing and forwarding (VRF) instance to a switch virtual interface (SVI).</p> <p>After the SVI is created, the VRF instance cannot be changed or unset. The VRF instance cannot be assigned to an internal SVI.</p>	No default
vrrp-virtual-mac {enable   disable}	Enable VRRP virtual MAC addresses for the IPv4 VRRP routers added to this interface. See RFC 5798 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 <ipv6_netmask>
    set ip6-allowaccess <access_types>
    set autoconf {disable | enable}
    set ip6-unknown-mcast-to-cpu {disable | enable}
    set ip6-mode {dhcp | static}
    set ip6-dns-server-override {disable | enable}
    set dhcp6-information-request {disable | enable}
    set ip6-send-adv {disable | enable}
    set ip6-manage-flag {disable | enable}
    set ip6-other-flag {disable | enable}
    set ip6-max-interval <4-1800>
    set ip6-min-interval <3-1350>
    set ip6-link-mtu <integer>
    set ip6-reachable-time <0-3600000>
    set ip6-retrans-time <0-2147483647>
    set ip6-default-life <0-9000>
    set ip6-hop-limit <0-255>
    set vrip6_link_local {enable | disable}
    set vrrp-virtual-mac6 {enable | disable}
    config ip6-extra-address
      edit <prefix_ipv6>
      next
    end
    config vrrp6
      edit <virtual_router_identififier 1-255>
        set accept-mode {enable | disable} ----Enable/disable accept mode. (enable by default)
        set adv-interval <1-255> ----Advertisement interval (1 - 255 seconds). (1 by default)
        set preempt {enable | disable} --Enable/disable preempt mode. (enable by default)
        set priority <1-255> --Priority of the virtual router (1 - 255). (100 by default)
        set start-time <1-255> --Startup time (1 - 255 seconds). (3 by default)
        set status {enable | disable} --Enable/disable VRRP. (enable by default)
        set vrdst6 <IPv6_address> ----Monitor the route to this destination. (no default)
        set vrgrp <1-65535> -----VRRP group ID (1 - 65535). (0 by default)
        set vrip6 <IPv6_address> ----IPv6 address of the virtual router. (no default) Required.
      next
    end
    config ip6-prefix-list
      edit <prefix_ipv6>
        set autonomous-flag {disable | enable}
        set onlink-flag {disable | enable}
        set preferred-life-time <0-2147483647>
        set valid-life-time <0-2147483647>
      end
    end
  end
end

```

Variable	Description	Default
<interface_name>	Edit an existing interface or create a new VLAN interface.	No default
ip6-address <ipv6_netmask>	The interface IPv6 address and netmask. The format for IPv6 addresses and netmasks is described in RFC 3513. This command is only available in NAT/Route mode.	::/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.
autoconf {disable   enable}	Enable or disable the automatic address configuration.	disable
ip6-unknown-mcast-to-cpu {disable   enable}	Enable or disable the sending of unknown multicast addresses to the CPU.	disable
ip6-mode {dhcp   static}	Set the addressing mode to be static or DHCP. DHCP addressing mode is available only when autoconf is disabled.	static
ip6-dns-server-override {disable   enable}	Enable or disable using the DNS server acquired by DHCP. This command is available only when the ip6-mode is set to dhcp.	enable
dhcp6-information-request {disable   enable}	Enable or disable the DHCPv6 information request.	disable
ip6-send-adv {disable   enable}	Enable or disable the sending of the IPv6 router advertisement. This command is only available when autoconf is disabled.	disable
ip6-manage-flag {disable   enable}	Enable or disable the sending of the IPv6 managed flag.	disable
ip6-other-flag {disable   enable}	Enable or disable the sending of the IPv6 other flag.	disable
ip6-max-interval <4-1800>	Specify the maximum number of seconds before the RA is sent.	600
ip6-min-interval <3-1350>	Specify the minimum number of seconds before the RA is sent.	198
ip6-link-mtu <integer>	Specify the IPv6 link maximum transmission unit.	0
ip6-reachable-time <0-3600000>	Specify the IPv6 reachable time in milliseconds.	0
ip6-retrans-time <0-2147483647>	Specify the IPv6 retransmit time in milliseconds.	0
ip6-default-life <0-9000>	Specify the IPv6 default life in seconds.	1800
ip6-hop-limit <0-255>	Specify the maximum number of IPv6 hops.	0

Variable	Description	Default
vrip6_link_local {enable   disable}	Enter the link-local IPv6 address of virtual router.	No default
vrrp-virtual-mac6 {enable   disable}	Enable VRRP virtual MAC addresses for the IPv6 VRRP routers added to this interface. See RFC 5798 for information about the VRRP virtual MAC addresses.	disable
<b>config ip6-extra-addr</b>		
<prefix_ipv6>	IPv6 address prefix. Configure additional IPv6 prefixes for this IPv6 interface.	No default
<b>config vrrp6</b>		
<virtual_router_identifier 1-255>	Enter the VRRP virtual router identifier. The range of values is 1-255.	No default
accept-mode {enable   disable}	Enable or disable the VRRP accept mode.	enable
adv-interval <1-255>	Enter the VRRP advertisement interval. The range of values is 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 <1-255>	Enter the priority of this virtual router. The VRRP virtual router on a network with the highest priority becomes the master. The range of values is 1-255.	100
start-time <1-255>	The startup time of this virtual router. The startup time is the maximum time that the backup system waits between receiving advertisement messages from the master system. The range of values is 1-255 seconds.	3
status {enable   disable}	Enable or disable this virtual router.	enable
vrdest6 <IPv6_address>	Monitor the route to this destination.	No default
vrgrp <1-65535>	Enter the VRRP group identifier. The value range is 1-65535.	0
vrip6 <IPv6_address>	Required. Enter the IPv6 address of the virtual router.	No default
<b>config ip6-prefix-list</b>		
<prefix_ipv6>	IPv6 advertised prefix list. Configure which IPv6 prefixes are advertised.	No default
autonomous-flag {disable   enable}	Enable or disable the autonomous flag.	enable
onlink-flag {disable   enable}	Enable or disable the onlink flag.	disable
preferred-life-time <0-2147483647>	Specify the preferred lifetime in seconds for the advertised IPv6 prefix.	604800

Variable	Description	Default
valid-life-time <0-2147483647>	Specify the valid lifetime in seconds for the advertised IPv6 prefix.	2592000

## Example

This example shows how to configure VRRP using IPv6:

```

config system interface
  edit "vlan30"
    set ip 30.0.0.5 255.255.255.0
    set allowaccess ping https http ssh telnet
    config vrrp
      edit 10
        set vrip 30.0.0.1
      next
    end
    set snmp-index 82
    config ipv6
      set ip6-address 2000::30:0:0:5/120
      config ip6-extra-addr
        edit 2000::30:3:3:5/120
        next
        edit 2000::30:3:4:5/120
        next
      end
      set ip6-allowaccess ping https http ssh telnet
      set vrrp-virtual-mac6 enable
      set vrip6_link_local fe80::30:0:0:1
      config vrrp6
        edit 10
          set vrip6 2000::30:0:0:1
        next
      end
    end
    set vlanid 30
    set interface "internal"
  next
end

config system interface
  edit "port26"
    set ip 30.44.0.5 255.255.255.0
    set allowaccess ping https http ssh telnet
    set type physical
    set l2-interface "port26"
    set vrrp-virtual-mac enable
    config vrrp
      edit 10
        set vrip 30.44.0.1
      next
    end
    set snmp-index 102
    config ipv6
      set ip6-address 2000::30:44:0:5/120

```

```

    set ip6-allowaccess ping https http ssh telnet
    set vrrp-virtual-mac6 enable
    set vrip6_link_local fe80::30:44:0:1
    config vrrp6
        edit 10
            set vrip6 2000::30:44:0:1
        next
    end
end
next
end

```

## config secondaryip

Configure a second IP address for the interface.

### Syntax

```

config system interface
edit <interface_name>
    config secondaryip
        edit <id>
            set ip <IP_address_and_netmask>
            set allowaccess <access_types>
        end
    end
end

```

Variable	Description	Default
<interface_name>	Edit an existing interface or create a new VLAN interface.	No default
<id>	Identifier.	No default
ip <IP_address_and_netmask>	Enter the IP address and netmask.	0.0.0.0 0.0.0.0
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.	No default

## config vrrp

Add one or more VRRP virtual routers to a interface. For information about VRRP, see RFC 5798.

### Syntax

```

config system interface
edit <interface_name>
    config vrrp
        edit <VRID_int>

```

```

    set adv-interval <seconds_int>
    set backup-vmac-fwd {enable | disable}
    set netmask <xxx.xxx.xxx.xxx>
    set preempt {enable | disable}
    set priority <prio_int>
    set start-time <seconds_int>
    set status {enable | disable}
    set version {2 | 3}
    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
<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
backup-vmac-fwd {enable   disable }	Enable or disable whether virtual MAC addresses are forwarded for VRRP backup.	enable
netmask <xxx.xxx.xxx.xxx>	Netmask of the virtual router.	0.0.0.0
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
version {2   3}	Set the VRRP version to VRRP version 2 or VRRP version 3.	2
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 ipv6-neighbor-cache

Use this command to configure the IPv6 neighbor cache table:

```

config system ipv6-neighbor-cache
edit <id>
    set interface {<string> | internal | mgmt}
    set ipv6 <IPv6_address>
    set mac <MAC_address>
end

```

Variable	Description	Default
<id>	Enter a unique integer to create a new entry.	No default
interface <interface_name>	Required. Enter the interface.	No default
ipv6 <IPv6_address>	Enter the IPv6 addresss in the following format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx	::
mac <MAC_address>	Enter the MAC address in the following format: xx:xx:xx:xx:xx:xx	00:00:00:00:00:00

### Example

This example shows how to configure an entry in the IPv6 neighbor cache table.

```

config system ipv6-neighbor-cache
edit id
    set interface internal
    set ipv6 e80::a5b:eff:fef1:95e4
    set mac 00:21:cc:d2:76:72
end

```

## config system link-monitor

Use this command to configure the link health monitor.

```
config system link-monitor
  edit <link monitor name>
    set addr-mode {ipv4 | ipv6}
    set srcintf <string>
    set server <IP_address1>, <IP_address2>, ...
    set protocol {arp | ping}
    set gateway-ip <IPv4 address>
    set gateway-ip6 <IPv6 address>
    set source-ip <IPv4 address>
    set source-ip6 <IPv6 address>
    set interval <integer>
    set timeout <integer>
    set failtime <integer>
    set recoverytime <integer>
    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
addr-mode {ipv4   ipv6}	Select whether to use IPv4 or IPv6 addresses.	ipv4
srcintf <string>	Interface where the monitor traffic is sent.	No default
server <IP_address1>, <IP_address2>, ..	The IP address(es) of the server(s). Use a comma to separate multiple IP addresses.	No default
protocol {arp   ping}	Protocols used to detect the server. Select ARP or ping.	ping
gateway-ip <IPv4 address>	Gateway IPv4 address used to PING the server. This option is available only when addr-mode is set to ipv4.	0.0.0.0
gateway-ip6 <IPv6 address>	Gateway IPv6 address used to PING the server. This option is available only when addr-mode is set to ipv6.	No default
source-ip <IPv4 address>	Source IPv4 address used in packet to the server. This option is available only when addr-mode is set to ipv4.	0.0.0.0
source-ip6 <IPv6 address>	Source IPv6 address used in packet to the server. This option is available only when addr-mode is set to ipv6.	No default
interval <integer>	Detection interval in seconds. The range is 1-3600.	5
timeout <integer>	Detect request timeout in seconds. The range is 1-255.	1
failtime <integer>	Number of retry attempts before bringing server down. The range is 1-10.	5
recoverytime <integer>	Number of retry attempts before bringing server up. The range is 1-10.	5

Variable	Description	Default
update-static-route {enable   disable}	Enable or disable update static route.	enable
status {enable   disable}	Enable or disable link monitor administrative status.	enable

## config system location

Use this command to configure the location table used by LLDP-MED for enhanced 911 emergency calls.

```

config system location
  edit <name>
    config address-civic
      set additional <string>
      set additional-code <string>
      set block <string>
      set branch-road <string>
      set building <string>
      set city <string>
      set city-division <string>
      set country <string>
      set country-subdivision <string>
      set county <string>
      set direction <string>
      set floor <string>
      set landmark <string>
      set language <string>
      set name <string>
      set number <string>
      set number-suffix <string>
      set place-type <string>
      set post-office-box <string>
      set postal-community <string>
      set primary-road <string>
      set road-section <string>
      set room <string>
      set script <string>
      set seat <string>
      set street <string>
      set street-name-post-mod <string>
      set street-name-pre-mod <string>
      set street-suffix <string>
      set sub-branch-road <string>
      set trailing-str-suffix <string>
      set unit <string>
      set zip <string>
    end
    config coordinates
      set altitude <string>
      set altitude-unit {f | m}
      set datum {NAD83 | NAD83/MLLW | WGS84}
      set latitude <string>
      set longitude <string>
  
```

```

end
config elin-number
  set elin-number <number>
end

```

Variable	Description	Default
<name>	Enter a unique name for the location entry.	No default
<b>config address-civic</b>		
additional <string>	Enter additional location information, for example, west wing.	No default
additional-code <string>	Enter the additional country-specific code for the location. In Japan, use the Japan Industry Standard (JIS) address code.	No default
block <string>	Enter the neighborhood (Korea) or block.	No default
branch-road <string>	Enter the branch road name. This value is used when side streets do not have unique names so that both the primary road and side street are used to identify the correct road.	No default
building <string>	Enter the name of the building (structure) if the address includes more than one building, for example, Law Library.	No default
city <string>	Enter the city (Germany), township, or shi (Japan).	No default
city-division <string>	Enter the city division, borough, city district (Germany), ward, or chou (Japan).	No default
country <string>	Enter the two-letter ISO 3166 country code in capital ASCII letters, for example, US, CA, DK, and DE.	No default
country-subdivision <string>	Enter the national subdivision (such as state, canton, region, province, or prefecture). In Canada, the subdivision is province. In Germany, the subdivision is state. In Japan, the subdivision is metropolis. In Korea, the subdivision is province. In the United States, the subdivision is state.	No default
county <string>	Enter the county (Canada, Germany, Korea, and United States), parish, gun (Japan), or district (India).	No default
direction <string>	Enter N, E, S, W, NE, NW, SE, or SW for the leading street direction.	No default
floor <string>	Enter the floor number, for example, 4.	No default
landmark <string>	Enter the nickname, landmark, or vanity address, for example, UC Berkeley.	No default
language <string>	Enter the ISO 639 language code used for the address information.	No default

Variable	Description	Default
name <string>	Enter the person or organization associated with the address, for example, Fortinet or Textures Beauty Salon.	No default
number <string>	Enter the street address, for example, 1560.	No default
number-suffix <string>	Enter any modifier to the street address. For example, if the full street address is 1560A, enter 1560 for the number and A for the number-suffix.	No default
place-type <string>	Enter the type of place, for example, home, office, or street.	No default
post-office-box <string>	Enter the post office box, for example, P.O. Box 1543. When the post-office-box value is set, the street address components are replaced with this value.	No default
postal-community <string>	Enter the postal community name, for example, Alviso. When the postal-community name is set, the civic community name is replaced by this value.	No default
primary-road <string>	Enter the primary road or street name for the address.	No default
road-section <string>	Enter the specific section or stretch of a primary road. This field is used when the same street number appears more than once on the primary road.	No default
room <string>	Enter the room number, for example, 7A.	No default
script <string>	Enter the script used to present the address information, for example, Latn.	No default
seat <string>	Enter the seat number in a stadium or theater or a cubicle number in an office or a booth in a trade show.	No default
street <string>	Enter the street (Canada, Germany, Korea, and United States).	No default
street-name-post-mod <string>	Enter an optional part of the street name that appears after the actual street name. If the full street name is East End Avenue Extended, the street-name-post-mod is Extended.	No default
street-name-pre-mod <string>	Enter an optional part of the street name that appears before the actual street name. If the full street name is Old North First Street, the street-name-pre-mod is Old.	No default
street-suffix <string>	Enter the type of street, for example, Ave or Place. Valid values are listed in the United States Postal Service Publication 28 [18], Appendix C.	No default

Variable	Description	Default
sub-branch-road <string>	Enter the name of a street that branches off of a branch road. This value is used when the primary road, branch road, and subbranch road names are needed to identify the correct street.	No default
trailing-str-suffix <string>	Enter N, E, S, W, NE, NW, SE, or SW for the trailing street direction.	No default
unit <string>	Enter the unit (apartment or suite), for example, Apt 27.	No default
zip <string>	Enter the postal or zip code for the address, for example, 94089-1345.	No default
<b>config coordinates</b>		
altitude <string>	Enter the vertical height of a location using the altitude-unit to specify the unit used. The format is +/- floating point number, for example, 117.47.	No default
altitude-unit {f   m}	Select whether the altitude is measured in m (meters) or f (floors).	m
datum {NAD83   NAD83/MLLW   WGS84}	Select which map is used for the location: WGS84, NAD83, or NAD83/MLLW.	WGS84
latitude <string>	Enter the latitude. The format is floating point starting with +/- or ending with N/S, for example, +/-16.67 or 16.67N.	No default
longitude <string>	Enter the longitude. The format is floating point starting with +/- or ending with E/W, for example, +/-26.789 or 26.789E.	No default
<b>config elin-number</b>		
elin-number <number>	Enter the emergency location identification number (ELIN), which is a unique phone number. The value is a 10 to 20 byte numerical string.	No default

## Example

This example shows how to configure the location table for Fortinet.

```
config system location
edit Fortinet
    config address-civic
        set country "US"
        set language "English"
        set county "Santa Clara"
        set city "Sunnyvale"
        set street "Kifer"
        set street-suffix "Road"
        set number "899"
        set zip "94086"
        set building "1"
```

```

        set floor "1"
        set seat "1293"
    end
next
edit "Fortinet"
    config elin-number
        set elin-number "14082357700"
    end
end
end

```

## config system ntp

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

### Syntax

```

config system ntp
    set allow-unsync-source {enable | disable}
    set authentication {enable | disable}
    set log-time-adjustments {enable | disable}
    set ntpsync {enable | disable}
    set source-ip <ipv4_addr>
    set source-ip6 <ipv6_addr>
    set syncinterval <interval_int>
    config ntpserver
        edit <serverid_int>
            set authentication {enable | disable}
            set key <string>
            set key-id <integer>
            set ntpv3 {enable | disable}
            set server {<ipv4_addr>| <ipv6_addr>}
        end
    end
end

```

Variable	Description	Default
allow-unsync-source {enable   disable}	Enable or disable whether an unsynchronized NTP server source is allowed.	disable
authentication {enable   disable}	Enable or disable authentication.	disable
log-time-adjustments {enable   disable}	Enable or disable whether FortiSwitch logs when NTP adjusts the system time.	enable
ntpsync {enable   disable}	Enable or disable whether the system time is synchronized with the NTP server.	enable
source-ip <ipv4_addr>	Enter the source IPv4 address for communication with the NTP server.	0.0.0.0
source-ip6 <ipv6_addr>	Enter the source IPv6 address for communication with the NTP server.	No default server.

Variable	Description	Default
syncinterval <interval_int>	Enter the interval in minutes between contacting the NTP server to synchronize time. The range is from 1 to 1,440 minutes. This option is available only when ntpsync is enabled.	10
<serverid_int>	Enter the number for this NTP server entry.	No default
authentication {enable   disable}	Enable or disable authentication. If you enable authentication and use the NTPv3 protocol, MD5 authentication is used. If you enable authentication and use the NTPv4 protocol, SHA1 authentication is used.	disable
key <string>	If authentication is enabled, enter a key for authentication.	No default
key-id <integer>	If authentication is enabled, enter a key identifier for authentication.	0
ntp3 {enable   disable}	Enable this option to use the NTPv3 protocol. Disable this option to use the NTPv4 protocol.	disable
server {<ipv4_addr>   <ipv6_addr>}	Enter the IPv4 or IPv6 address for this NTP server.	No default

## Example

This example shows how to configure an NTP server:

```
config system ntp
  set authentication enable
  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
  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	Enable password policy. The password policy cannot be disabled.	enable
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
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 ptp interface-policy

Use this command to configure the default Precision Time Protocol (PTP) policy or create a custom PTP policy.

### Syntax

```
config system ptp interface-policy
  edit {default | PTP_policy_name}
    set description <description_of_PTP_policy>
    set vlan <0-4094>
    set vlan-pri <0-7>
  next
end
```

Parameter	Description	Default value
{default   PTP_policy_name}	Name of the PTP policy.	default
description <description_of_PTP_policy>	Description of the PTP policy.	No default
vlan <0-4094>	The VLAN that will use the PTP policy. The range of values is 0-4094. Setting <code>vlan</code> to 0 means that the native VLAN is used for PDelayXXX messages. <b>NOTE:</b> The VLAN must be a valid VLAN that the interface belongs to. Selecting an invalid VLAN can affect the performance.	0
vlan-pri <0-7>	The priority of the PTP VLAN; it corresponds to the 802.1p priority. The VLAN priority is used only when there is traffic congestion. The range of values is 0-7. Set <code>vlan-pri</code> to 7 for the highest priority.	4

### Example

This example shows how to create a custom PTP policy:

```
config system ptp interface-policy
  edit newPTPpolicy
    set description "PTP policy for VLAN 100"
    set vlan 100
    set vlan-pri 3
  next
end
```

## config system ptp profile

Use this command to configure a PTP profile.

## Syntax

```

config system ptp profile
  edit {default | name_of_PTP_profile}
    set announce-interval {0.25sec | 0.5sec | 1sec | 2sec | 4sec}
    set announce-timeout <2-10>
    set description <description_of_PTP_profile>
    set domain <0-255>
    set min-delay-req-interval {0.25sec | 0.5sec | 1sec | 2sec | 4sec}
    set mode {boundary-e2e | boundary-p2p | transparent-e2e | transparent-p2p}
    set pdelay-req-interval {0.25sec | 0.5sec | 1sec | 2sec | 4sec}
    set priority1 <0-255>
    set priority2 <0-255>
    set ptp-profile {default | C37.238-2017}
    set sync-interval {0.25sec | 0.5sec | 1sec | 2sec | 4sec}
    set transport l2-mcast
  next
end

```

Parameter	Description	Default value in end-to-end mode	Default value in peer-to-peer mode
{default   name_of_PTP_profile}	Name of the PTP profile.	No default	No default
announce-interval {0.25sec   0.5sec   1sec   2sec   4sec}	Select the number of seconds between Announce messages. This option is available only when mode is set to boundary-e2e or boundary-p2p.	1sec	1sec
announce-timeout <2-10>	Select how many seconds before the PTP Announce message expires. This option is available only when mode is set to boundary-e2e or boundary-p2p.	3	3
description <description_of_PTP_profile>	Description of the PTP profile.	No default	No default
domain <0-255>	PTP domain number. The range of values is 0-255. This option is available only when mode is set to transparent-p2p, boundary-e2e, or boundary-p2p.	1	For the transparent clock, the default value is 1 if using the default PTP profile or 254 if using the power PTP profile.

Parameter	Description	Default value in end-to-end mode	Default value in peer-to-peer mode
min-delay-req-interval {0.25sec   0.5sec   1sec   2sec   4sec}	Select the number of seconds between Delay_Req messages.  This option is available only when mode is set to boundary-e2e.	1sec	Not applicable
mode {boundary-e2e   boundary-p2p   transparent-e2e   transparent-p2p}	PTP mode. You can select from the following modes: <ul style="list-style-type: none"> <li>boundary-e2e—Boundary clock using the end-to-end mode.</li> <li>boundary-p2p—Boundary clock using the peer-to-peer mode.</li> <li>transparent-e2e—Transparent clock using the end-to-end mode.</li> <li>transparent-p2p—Transparent clock using the peer-to-peer mode.</li> </ul>	transparent-e2e	Not applicable. You need to create a profile and set the mode to boundary-p2p or transparent-p2p.
pdelay-req-interval {0.25sec   0.5sec   1sec   2sec   4sec}	The time between PDelay_Req messages. You can select 0.25, 0.5, 1, 2, or 4 seconds. The default value is 1 second.  This option is available only when mode is set to transparent-p2p or boundary-p2p.	Not applicable	1sec
priority1 <0-255>	Set the PTP priority 1. Use a smaller number for a higher priority.  This option is available only when mode is set to boundary-e2e or boundary-p2p.	128	128
priority2 <0-255>	Set the PTP priority 2. Use a smaller number for a higher priority.  This option is available only when mode is set to boundary-e2e or boundary-p2p.	128	128
ptp-profile {default   C37.238-2017}	PTP profile. Select default for the IEEE 1588 default profile or C37.238-2017 for the power profile.  C37.238-2017 is available only when mode is set to transparent-p2p.	default	default
sync-interval {0.25sec   0.5sec   1sec   2sec   4sec}	Select how many seconds between clock synchronization.	1sec	1sec

Parameter	Description	Default value in end-to-end mode	Default value in peer-to-peer mode
transport l2-mcast	PTP message transmission. This option is available only when mode is set to transparent-p2p, boundary-e2e, or boundary-p2p.	Layer-2 and layer-3 multicast are supported for end-to-end transparent clock. All other modes support layer-2 multicast only.	Layer-2 multicast

## Example

This example shows how to configure a PTP profile:

```
config system ptp profile
  edit newprofile
    set description "New PTP profile"
    set domain 1
  next
end
```

## config system schedule group

Use this command to define a schedule group. A schedule group can contain both one-time schedules and recurring schedules. To create one-time and recurring schedules, see [config system schedule onetime on page 251](#) and [config system schedule recurring on page 251](#).

### Syntax

```
config system schedule group
  edit <schedule_group_name>
    set member <schedule_name1> <schedule_name2> ...
  end
```

Variable	Description	Default
<schedule_group_name>	Enter the name of the schedule group.	No default
member <schedule_name1> <schedule_name2> ...	Enter the names of the schedules to include. Separate multiple names with a space.  The schedules must already be defined with the <a href="#">config system schedule onetime</a> or <a href="#">config system schedule recurring</a> command.	No default

## Example

This example shows how to create a schedule group:

```
config system schedule group
  edit group1
```

```

    set member schedule1 schedule2
end

```

## config system schedule onetime

Use this command to define a one-time schedule for when a policy will be enforced.

### Syntax

```

config system schedule onetime
  edit <schedule_name>
    set start <time_date>
    set end <time_date>
  end

```

Variable	Description	Default
<schedule_name>	Enter the name of the schedule.	No default
start <time_date>	Enter the start time and date for the schedule in the following format: hh:mm yyyy/mm/dd	00:00 1900/01/01
end <time_date>	Enter the end time and date for the schedule in the following format: hh:mm yyyy/mm/dd	00:00 1900/01/01

### Example

This example shows how to create a one-time schedule:

```

config system schedule onetime
  edit schedule1
    set start 07:00 2019/03/22
    set end 07:00 2019/03/29
  end

```

## config system schedule recurring

Use this command to define a schedule for specified hours every week.

### Syntax

```

config system schedule recurring
  edit <schedule_name>
    set day {monday | tuesday | wednesday | thursday | friday | saturday | sunday}
    set start <time>
    set end <time>
  end

```

Variable	Description	Default
<schedule_name>	Enter the name of the schedule.	No default
day {monday   tuesday   wednesday   thursday   friday   saturday   sunday}	Enter one or more days for the ACL to be enforced. Separate days with a space.	monday tuesday wednesday thursday friday
start <time>	Enter the start time for the schedule in the following format: hh:mm	24:00
end <time>	Enter the end time for the schedule in the following format: hh:mm	24:00

## Example

This example shows how to create a recurring schedule:

```
config system schedule recurring
  edit schedule2
    set day monday wednesday friday
    set start 07:00
    set end 08:00
  end
```

## config system settings

Use this command 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 ip-ecmp-mode {source-ip-based | dst-ip-based | port-based}
end
```

Variable	Description	Default
ip-ecmp-mode {source-ip-based   dst-ip-based   port-based}	Select the IPv4 ECMP mode: <ul style="list-style-type: none"> <li>dst-ip-based – Select the next hop based on the destination IP address.</li> <li>port-based – Select the next hop based on the TCP/UDP port.</li> <li>source-ip-based – Select the next hop based on the source IP address.</li> </ul>	source-ip-based

### Example

This example shows how to configure ECMP:

```
config system settings
    set ip-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 sFlow collectors.

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 sFlow collectors.

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 collectors to show traffic flows and patterns.

### Syntax

```
config system sflow
    config collectors
        edit <collector_name>
            set ip <collector_IPv4_address>
            set port <collector_port>
        next
    end
end
```

Variable	Description	Default
<collector_name>	Enter a name for the sFlow collector.	No default
ip <collector_IPv4_address>	The sFlow agents send sFlow datagrams to the sFlow collector at this IPv4 address.	0.0.0.0
port <collector_port>	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
  config collectors
    edit collector1
      set ip 20.20.20.0
      set port 200
    next
  end
end
```

## config system sniffer-profile

Use this command to define a packet-capture profile to select which packets to examine. To start, stop, and pause the packet capture, see the `execute system sniffer-profile` commands.

### Syntax

```
config system sniffer-profile
  edit <profile_name>
    set filter {<string> | none}
    set max-pkt-count <1-maximum>
    set max-pkt-len <64-1534>
    set switch-interface <switch_interface_name>
    set system-interface <system_interface_name>
  end
```

Variable	Description	Default
<profile_name>	The name of the packet-capture profile.	No default
filter {<string>   none}	Enter none or enter the filter for selecting which packets to capture. For example, if you want packets using UDP port 1812 between hosts named <code>forti1</code> and either <code>forti2</code> or <code>forti3</code> : 'udp and port 1812 and host <code>forti1</code> and \( <code>forti2</code> or <code>forti3</code> \)'	none
max-pkt-count <1-maximum>	Enter how many packets to be captured on the selected interface. The maximum number of packets that can be captured differs according to platform. See the <i>FortiSwitchOS Administration Guide</i> for details.	4000
max-pkt-len <64-1534>	Enter the maximum packet length in bytes to be captured on the interface.	128
switch-interface <switch_interface_name>	Enter the switch interface name that you want to capture packets on. You cannot select both a switch interface and a system interface.	No default
system-interface <system_interface_name>	Enter the system interface name that you want to capture packets on. You cannot select both a switch interface and a system interface.	No default

## Example

This example shows how to create a packet-capture profile:

```
config system sniffer-profile
  edit profile1
    set filter none
    set max-pkt-count 100
    set max-pkt-len 100
    set system-interface mgmt
  end
```

## config system snmp community

Use this command to configure SNMP communities on your FortiSwitch unit.

### 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 <interface_name>
      set ip <IPv4_address/mask>
      set source-ip <IPv4_address>
    end
  config hosts6
    edit <host_number>
      set interface <interface_name>
      set ip6 <IPv6_address>
      set source-ip6 <IPv6_address>
    end
  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

Variable	Description	Default
events <events_list>	<p>Enable the events for which the system should send traps to the SNMP managers in this community. The following events can be enabled:</p> <ul style="list-style-type: none"> <li>• <code>cpu-high</code>—The CPU usage is too high.</li> <li>• <code>ent-conf-change</code>—The entity's configuration was changed (RFC 4133).</li> <li>• <code>fan-detect</code>—The fan was detected, not detected, resumed, or failed.</li> <li>• <code>fsTrapStitch1</code>—Custom SNMP trap 1. Use this event as a trigger for an automation stitch.</li> <li>• <code>fsTrapStitch2</code>—Custom SNMP trap 2. Use this event as a trigger for an automation stitch.</li> <li>• <code>fsTrapStitch3</code>—Custom SNMP trap 3. Use this event as a trigger for an automation stitch.</li> <li>• <code>fsTrapStitch4</code>—Custom SNMP trap 4. Use this event as a trigger for an automation stitch.</li> <li>• <code>fsTrapStitch5</code>—Custom SNMP trap 5. Use this event as a trigger for an automation stitch.</li> <li>• <code>intf-ip</code>—The interface's IP address was changed.</li> <li>• <code>ip-conflict</code>—There is a conflict between IP addresses.</li> <li>• <code>l2mac</code>—A layer-2 MAC address has been added, deleted, or moved. <b>NOTE:</b> This SNMP trap applies only to dynamic MAC addresses learned on the port. MAC events can be lost by the hardware or software.</li> <li>• <code>llv</code>—Learning-limit violation.</li> <li>• <code>log-full</code>—The available log space is low.</li> <li>• <code>mem-low</code>—The available memory is low.</li> <li>• <code>psu-status</code>—The status of the power supply unit has changed.</li> <li>• <code>sensor-alarm</code>—The sensor triggered an alarm.</li> <li>• <code>sensor-fault</code>—The sensor is faulty.</li> <li>• <code>storm-control</code>—There has been a change in the storm-control status. <b>NOTE:</b> You must specify one or more IP addresses of the host(s) to monitor.</li> <li>• <code>tkmem-hb-oo-sync</code>—The trunk member's heart beat is unsynchronized.</li> </ul>	All events enabled, except for <code>l2mac</code> .
name <community_name>	<p>Enter the name of the SNMP community.</p> <p><b>NOTE:</b> After you run the <code>execute factoryreset</code> command, FortiSwitchOS creates an SNMP community with the name set to <code>public</code>.</p>	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

Variable	Description	Default
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
<b>config hosts and hosts6</b>		
<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 <interface_name>	Enter the name of the FortiSwitch interface to which the SNMP manager connects.	No default
ip <IPv4_address/mask>	Enter the IPv4 IP address and mask of the SNMP manager (for hosts).	0.0.0.0
ip6 <IPv6_address>	Enter the IPv6 IP address of the SNMP manager (for hosts6).	::
source-ip <IPv4_address>	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 <IPv6_address>	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 unit, 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-interval {1min | 10min | 30min | 1hr | 12hr | 24hr}
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 unit. 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
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: <ul style="list-style-type: none"> <li>• Fortinet prefix 0x8000304404</li> <li>• the optional engine-id string, 24 characters maximum, defined in this command</li> </ul> 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-interval {1min   10min   30min   1hr   12hr   24hr}	Set how long the FortiSwitch CPU usage must be higher than the specified threshold before an SNMP v3 notification (trap) is reported.	1min
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

Variable	Description	Default
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 auth-proto {md5 | sha1 | sha224 | sha256 | sha384 | sha512}
    set auth-pwd <password>
    set events {events_list}
    set notify-hosts <IP_address>
    set priv-proto {aes128 | aes192 | aes192c | aes256 | aes256c | des}
    set priv-pwd <password>
    set queries {enable | disable}
    set query-port <port_int>
    set security-level {no-auth-no-priv | auth-no-priv | auth-priv}
  end
```

Variable	Description	Default
<user_name>	Edit or add selected user.	No default
auth-proto {md5   sha1   sha224   sha256   sha384   sha512}	Select the authentication protocol. <ul style="list-style-type: none"> <li>md5—HMAC-MD5-96 authentication protocol</li> <li>sha1—HMAC-SHA-1 authentication protocol</li> <li>sha224—HMAC-SHA-224 authentication protocol</li> <li>sha256—HMAC-SHA-256 authentication protocol</li> <li>sha384—HMAC-SHA-384 authentication protocol</li> <li>sha512—HMAC-SHA-512 authentication protocol</li> </ul> This option is available only when security-level is set to	sha1

Variable	Description	Default
	auth-priv or auth-no-priv.	
auth-pwd <password>	Enter the password for the authentication protocol. This option is available only when security-level is set to auth-priv or auth-no-priv.	No default
events {events_list}	Specify one or more SNMP notifications (traps) to send. Separate multiple values with a space. The following notifications are available: <ul style="list-style-type: none"> <li>cpu-high—The CPU usage is too high.</li> <li>ent-conf-change—The entity's configuration was changed (RFC 4133).</li> <li>fan-detect—The fan was detected, not detected, resumed, or failed.</li> <li>fsTrapStitch1—Custom SNMP trap 1. Use this event as a trigger for an automation stitch.</li> <li>fsTrapStitch2—Custom SNMP trap 2. Use this event as a trigger for an automation stitch.</li> <li>fsTrapStitch3—Custom SNMP trap 3. Use this event as a trigger for an automation stitch.</li> <li>fsTrapStitch4—Custom SNMP trap 4. Use this event as a trigger for an automation stitch.</li> <li>fsTrapStitch5—Custom SNMP trap 5. Use this event as a trigger for an automation stitch.</li> <li>intf-ip—The interface's IP address was changed.</li> <li>ip-conflict—There is a conflict between IP addresses.</li> <li>l2mac—A layer-2 MAC address has been added, deleted, or moved. <b>NOTE:</b> This SNMP trap applies only to dynamic MAC addresses learned on the port. MAC events can be lost by the hardware or software.</li> <li>llv—Learning-limit violation.</li> <li>log-full—The available log space is low.</li> <li>mem-low—The available memory is low.</li> <li>psu-status—The status of the power supply unit has changed.</li> <li>sensor-alarm—The sensor triggered an alarm.</li> <li>sensor-fault—The sensor is faulty.</li> <li>storm-control—There has been a change in the storm-control status.</li> <li>tkmem-hb-oo-sync—The trunk member's heart beat is unsynchronized.</li> </ul>	All events enabled, except for l2mac.
notify-hosts <IP_address>	Specify one or more IPv4 addresses to send notifications (traps) to.	No default

Variable	Description	Default
priv-prot {aes128   aes192   aes192c   aes256   aes256c   des}	Select the encryption protocol. <ul style="list-style-type: none"> <li>aes128—CFB128-AES-128 symmetric encryption protocol</li> <li>aes192—CFB128-AES-192 symmetric encryption protocol</li> <li>aes192c—CFB128-AES-192-C symmetric encryption protocol (required for certain clients)</li> <li>aes256—CFB128-AES-256 symmetric encryption protocol</li> <li>aes256c—CFB128-AES-256-C symmetric encryption protocol (required for certain clients)</li> <li>des—CBC-DES symmetric encryption protocol</li> </ul> This option is available only when security-level is set to auth-priv.	aes128
priv-pwd <password>	Enter the password for the encryption protocol. This option is available only when security-level is set to auth-priv.	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 {no-auth-no-priv   auth-no-priv   auth-priv}	Set the security level to one of: <ul style="list-style-type: none"> <li>no-auth-no-priv—no authentication or privacy</li> <li>auth-no-priv—authentication but no privacy</li> <li>auth-priv—authentication and privacy</li> </ul>	no-auth-no-priv

## config system vxlan

Use this command to configure VXLAN interfaces.

### Syntax

```
config system vxlan
  edit <VXLAN_interface_name>
    set vni <integer>
    set vlanid <integer>
    set evpn {disable | enable}
    set arp-nd-suppression {disable | enable}
    set interface <interface_name>
    set ip-version {ipv4-multicast | ipv4-unicast}
    set remote-ip <IPv4_address>
    set tagged-vlans <VLAN_list>
    set tunnel-loopback <interface_name>
  next
end
```

Variable	Description	Default
<VXLAN_interface_name>	Enter a name for the VXLAN interface	No default
vni <integer>	Required. Set the VXLAN network identifier (VNI). The range of values is 1-16777215.	0
vlanid <integer>	Required. Set the VLAN identifier that is mapped to the VNI. When tunnel-loopback is set, VLAN 4087 is reserved.	0
evpn {disable   enable}	Enable or disable the Ethernet Virtual Private Network (EVPN).	disable
arp-nd-suppression {disable   enable}	Enable or disable ARP and ND suppression. This command is available only when evpn is enabled.	disable
interface <interface_name>	Required. Enter the name of the outgoing interface for the VXLAN tunnel. Starting in FortiSwitchOS 7.2.1, you can specify a routed VLAN interface (RVI).	No default
ip-version {ipv4-multicast   ipv4-unicast}	Required. Select the type of IPv4 address to use to communicate over the VXLAN tunnel. <ul style="list-style-type: none"> <li>• ipv4-multicast—Use IPv4 multicast addressing over the VXLAN tunnel.</li> <li>• ipv4-unicast—Use IPv4 unicast addressing over the VXLAN tunnel.</li> </ul>	ipv4-unicast
remote-ip <IPv4_address>	Required. Enter the source and destination IPv4 addresses of the VXLAN interface. The VXLAN tunnel destination must match the remote-ip setting of the VXLAN tunnel initiator. Starting in FortiSwitchOS 7.2.1, you can specify an RVI as the source or destination IPv4 address.	No default
tagged-vlans <VLAN_list>	User traffic is sent with the specified inner VLAN tags. This command is available only when the switch is managed by a FortiGate device.	No default
tunnel-loopback <interface_name>	Enter the name of the tunnel-loopback interface. The tunnel-loopback can be set only on FS-1024E, FS-T1024E, and FS-1048E. When tunnel-loopback is set, VLAN 4087 is reserved. This command is available only when the switch is managed by a FortiGate device.	No default

## Example

This example shows how to configure a VXLAN interface:

```
config system vxlan
  edit "newvxlan"
    set vni 50
    set vlanid 50
    set interface "vlan40"
    set remote-ip "1.2.3.4" "5.6.7.8"
  next
end
```

## config system web

Use this command to configure web attributes.

### Syntax

```
config system web
  set gui-language {browser | english | french | german | japanese | korean | portuguese | simch |
    spanish | trach}
  set http-port <1-65535>
  set https-pki-required {enable | disable}
  set https-port <1-65535>
  set https-server-cert {self-sign | Fortinet_802.1x | Fortinet_Factory | Fortinet_Factory2 |
    Fortinet_Firmware}
  set https-ssl-versions {tlsv1-1 | tlsv1-2 | tlsv1-3}
end
```

Variable	Description	Default
gui-language {browser   english   french   german   japanese   korean   portuguese   simch   spanish   trach}	Set the display language to the language used in the browser (browser), English, French, German, Japanese, Korean, Portuguese, simplified Chinese (simch), Spanish, or traditional Chinese(trach).	browser
http-port <1-65535>	Enter the port to use for HTTP administrative access.	80
https-pki-required {enable   disable}	Enable to allow users to log in 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
https-port <1-65535>	Enter the port to use for HTTPS administrative access.	443

Variable	Description	Default
https-server-cert {self-sign   Fortinet_802.1x   Fortinet_Factory   Fortinet_Factory2   Fortinet_Firmware}	Select the administration HTTPS server certificate to use: <ul style="list-style-type: none"> <li>• <code>self-sign</code>—Use a self-signed security certificate. Self-signed certificates are free and will encrypt the data just as securely as a purchased certificate. Self-signed certificates, however, are not likely to be recognized by the CA certificate store so will be considered by any checks against that store as invalid.</li> <li>• <code>Fortinet_802.1x</code>—This certificate is embedded in the firmware and is the same on every unit (not unique). It has been signed by a public CA.</li> <li>• <code>Fortinet_Factory</code>—This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.</li> <li>• <code>Fortinet_Factory2</code>—This certificate is embedded in the hardware at the factory and is unique to this unit. It has been signed by a proper CA.</li> <li>• <code>Fortinet_Firmware</code>—This certificate is embedded in the firmware and is the same on every unit (not unique). It has been signed by a proper CA. It is not recommended to use it for server-type functionality since any other unit could use this same certificate to spoof the identity of this unit.</li> </ul>	Fortinet_Firmware
https-ssl-versions {tls1-1   tls1-2   tls1-3}	Set the allowed SSL/TLS versions for web administration.	tls1-1 tls1-2 tls1-3

## 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 on page 264](#)
- [config user ldap on page 266](#)
- [config user local on page 268](#)
- [config user peer on page 269](#)
- [config user peergrp on page 270](#)
- [config user radius on page 270](#)
- [config user setting on page 274](#)
- [config user tacacs+ on page 276](#)

## 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
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: <ul style="list-style-type: none"> <li>firewall - FortiSwitch users defined in user local, user ldap or user radius</li> <li>fsso-service - Directory Service users</li> </ul>	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
<b>config match</b>		
<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 unit, 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 unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiSwitch unit.

### Syntax

```

config user ldap
  edit <server_name>
    set cnid <id>
    set dn <dnname>
    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>
    set ca-cert <CA_certificate_name>
    set server-identity-check {enable | disable}
  next
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 <dnname>	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

Variable	Description	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
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 following 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: <ul style="list-style-type: none"> <li>• disable – port 389</li> <li>• ldaps – port 636</li> <li>• starttls – port 389</li> </ul>	disable
ca-cert <CA_certificate_name>	Select the CA certificate to use.	No default
server-identity-check {enable   disable}	Enable or disable whether the LDAP server identity is checked. If this option is enabled, FortiSwitchOS verifies the server domain name and IP address against the server certificate. <b>NOTE:</b> To enable this option, set secure to ldaps and select a CA certificate for ca-cert.	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 unit.	enable
type <auth-type>	Enter one of the following to specify how this user's password is verified: <ul style="list-style-type: none"> <li>ldap: The LDAP server specified in ldap-server verifies the password.</li> <li>password: The system verifies the password against the value of the password.</li> <li>radius: The RADIUS server specified in radius-server verifies the password.</li> </ul>	No default

Variable	Description	Default
	<ul style="list-style-type: none"> <li>tacacs+: The TACACS+ server specified in tacacs+-server verifies the password.</li> </ul>	

## config user peer

Use this command to configure a peer user.

### Syntax

```
config user peer
  edit <peer_name>
    set ca {Entrust_802.1x_CA | Entrust_802.1x_G2_CA | Entrust_802.1x_L1K_CA | Fortinet_CA | Fortinet_CA2}
    set cn <string>
    set cn-type {FQDN | email | ipv4 | ipv6 | string}
    set ldap-mode {password | principal-name}
    set ldap-password <password>
    set ldap-server <string>
    set ldap-username <string>
    set mandatory-ca-verify {enable | disable}
    set passwd <password>
    set subject <string>
    set two-factor {enable | disable}
  next
end
```

Variable	Description	Default
<peer_name>	Enter the name of the peer user.	No default
ca {Entrust_802.1x_CA   Entrust_802.1x_G2_CA   Entrust_802.1x_L1K_CA   Fortinet_CA   Fortinet_CA2}	Select a certificate authority (CA) for the peer certificate.	No default
cn <string>	Enter the common name for the peer certificate.	No default
cn-type {FQDN   email   ipv4   ipv6   string}	Enter the type of common name for the peer certificate: fully qualified domain name, email address, IPv4 address, IPv6 address, or a text description.	string
ldap-mode {password   principal-name}	Select whether the peer LDAP requires a password or an email address. The password is specified with the set ldap-password command.	password
ldap-password <password>	Enter the password for the peer LDAP. This option is available only when the ldap-mode is set to password.	No default

Variable	Description	Default
ldap-server <string>	Enter the name of the LDAP server used for checking access permission.	No default
ldap-username <string>	Enter the user name for the LDAP server.	No default
mandatory-ca-verify {enable   disable}	Enable or disable whether there is mandatory CA verification.	disable
passwd <password>	Enter the user password for two-factor authentication. This option is available only when two-factor is enabled.	No default
subject <string>	Enter any limitations on the peer certificate name.	No default
two-factor {enable   disable}	Enable or disable two-factor authentication. When this option is enabled, the certificate and password are required. Specify the password in the set passwd command.	disable

## config user peergrp

Use this command to configure a peer user group.

### Syntax

```
config user peergrp
  edit <peer_group_name>
    set member <list_of_peer_names>
  next
end
```

Variable	Description	Default
<peer_group_name>	Enter a name for the new peer group.	No default
<list_of_peer_names>	Enter one or more peer users. Separate the names with a space. The peer users must already be configured with the config user peer command before they are added to a peer user group.	No default

## config user radius

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

### Syntax

```
config user radius
  edit <RADIUS_user_name>
    set acct-fast-framedip-detect <integer>
    set acct-interim-interval <integer>
    set addr-mode {ipv4 | ipv6}
```

```

set all-usergroup {enable | disable}
set auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}
set frame-mtu-size <integer>
set link-monitor {enable | disable}
set link-monitor-interval <5-120>
set nas-ip <use_ip>
set nas-ip6 <ipv6_addr>
set radius-coa {enable | disable}
set radius-port <radius_port_num>
set secret <server_password>
set server <domain_ipv4_ipv6>
set service-type {administrative | authenticate-only | call-check | callback-administrative |
  callback-framed | callback-login | callback-nas-prompt | framed | login | nas-prompt |
  outbound}
set source-ip <ipv4_addr>
set source-ip6 <ipv6_addr>
config acct-server
  edit <accounting_server_ID>
    set status {enable | disable}
    set server <accounting_server>
    set secret <accounting_server_secret>
    set port <accounting_server_port>
  next
end
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
acct-fast-framedip-detect <integer>	Enter the number of seconds allowed for the first-time detection of the Framed-IP-Address attribute from DHCP snooping. The range is 2-600 seconds.	2
acct-interim-interval <integer>	Enter the number of seconds between each interim accounting message sent to the RADIUS server. The value range is 60-86400.	600
addr-mode {ipv4   ipv6}	Select whether to connect to the RADIUS server with IPv4 or IPv6. <b>NOTE:</b> If you select ipv4, you must use an IPv4 address for the set server command. If you select ipv6, you must use an IPv6 address for the set server command.	ipv4
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
frame-mtu-size <integer>	Enter the maximum frame size in octets used to advertise to the authentication server. The range is 600-1500.	1500
link-monitor {enable   disable}	Enable or disable whether this server sends periodic ping messages to the RADIUS server to test if it is available.	disable

Variable	Description	Default
link-monitor-interval <5-120>	Enter how often (in seconds) the server checks if the RADIUS server is available.	15
nas-ip <use_ip>	IPv4 address used as NAS-IP-Address and Called-Station-ID attribute in RADIUS access requests. RADIUS setting or IPv4 address of FortiGate interface used to talk with RADIUS server, if not configured. This option is available when the addr-mode is set to ipv4.	No default
nas-ip6 <ipv6_addr>	IPv6 address used as NAS-IPv6-Address and Called-Station-ID attribute in RADIUS access requests. RADIUS setting or IPv6 address of FortiGate interface used to talk with RADIUS server, if not configured. This option is available when the addr-mode is set to ipv6.	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_ipv4_ipv6>	Enter the RADIUS server domain name, IPv4 address, or IPv6 address. <b>NOTE:</b> If you selected <code>ipv4</code> for <code>addr-mode</code> , you must use an IPv4 address for the <code>set server</code> command. If you selected <code>ipv6</code> for <code>addr-mode</code> , you must use an IPv6 address for the <code>set server</code> command.	No default
source-ip <ipv4_addr>	Enter the source IPv4 address for communicating to the RADIUS server. This option is available when the addr-mode is set to ipv4.	0.0.0.0
source-ip6 <ipv6_addr>	Enter the source IPv6 address for communicating to the RADIUS server. This option is available when the addr-mode is set to ipv6.	No default
<b>config acct-server</b>		
<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
secret <accounting_server_secret>	Enter the shared secret key for the RADIUS accounting server.	*
server <accounting_server>	Enter the RADIUS server domain name, IPv4 address, or IPv6 address of the RADIUS server that will be receiving the accounting messages.	No default

Variable	Description	Default
service-type {administrative   authenticate-only   call-check   callback-administrative   callback-framed   callback-login   callback-nas-prompt   framed   login   nas-prompt   outbound}	Select the Service-Type value. Separate multiple values with a space.	none
port <accounting_server_port>	Enter the port number for the RADIUS accounting server to receive accounting messages from the FortiSwitch unit.	1813

## 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.

## 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 connect to a RADIUS server using IPv4:

```
config user radius
```

```
edit "local-RADIUS"
  set addr-mode ipv4
  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
    next
  end
next
end
```

This example shows how to connect to a RADIUS server using IPv6:

```
config user radius
  edit "radius"
    set acct-interim-interval 60
    config acct-server
      edit 1
        set status enable
        set server "ipv6local"
        set secret djfhde;rkjfkrekdfjeke
      next
    end
    set radius-coa enable
    set secret djfhde;rkjfkrekdfjeke
    set server "ipv6local"
    set service-type login callback-nas-prompt
    set addr-mode ipv6
    set nas-ip6 4001:1:2::1
    set source-ip6 4001:1:2::1
  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
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
<b>config auth-ports</b>		

Variable	Description	Default
<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>
  end
```

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 automation test on page 280](#)
- [diagnose bpdu-guard display status on page 280](#)
- [diagnose certificate all on page 281](#)
- [diagnose certificate ca on page 283](#)
- [diagnose certificate local on page 284](#)
- [diagnose certificate remote on page 284](#)
- [diagnose debug application on page 285](#)
- [diagnose debug authd on page 287](#)
- [diagnose debug bfd on page 288](#)
- [diagnose debug bgp on page 288](#)
- [diagnose debug cli on page 288](#)
- [diagnose debug config-error-log on page 288](#)
- [diagnose debug console on page 289](#)
- [diagnose debug crashlog on page 289](#)
- [diagnose debug disable on page 290](#)
- [diagnose debug enable on page 291](#)
- [diagnose debug info on page 291](#)
- [diagnose debug isis on page 291](#)
- [diagnose debug kernel level on page 291](#)
- [diagnose debug ospf on page 292](#)
- [diagnose debug ospf6 on page 292](#)
- [diagnose debug packet\\_test on page 292](#)
- [diagnose debug pbr on page 293](#)
- [diagnose debug pim on page 293](#)
- [diagnose debug port-mac on page 293](#)
- [diagnose debug report on page 294](#)
- [diagnose debug reset on page 295](#)
- [diagnose debug rip on page 295](#)
- [diagnose debug ripng on page 296](#)
- [diagnose debug static on page 296](#)
- [diagnose debug unit\\_test on page 296](#)
- [diagnose debug zebra on page 296](#)
- [diagnose firewall ip clear-counter on page 296](#)
- [diagnose firewall ip show on page 297](#)
- [diagnose firewall ipv6 clear-counter on page 297](#)
- [diagnose firewall ipv6 show on page 297](#)
- [diagnose flapguard status on page 297](#)
- [diagnose hardware on page 299](#)
- [diagnose ip address on page 302](#)

- [diagnose ip arp on page 303](#)
- [diagnose ip route on page 303](#)
- [diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra} on page 305](#)
- [diagnose ip router command on page 306](#)
- [diagnose ip router fwd on page 306](#)
- [diagnose ip router process show on page 307](#)
- [diagnose ip router terminal-monitor on page 308](#)
- [diagnose ip rules list on page 308](#)
- [diagnose ip rcache list on page 308](#)
- [diagnose ip tcp on page 308](#)
- [diagnose ip udp on page 309](#)
- [diagnose ipv6 address on page 310](#)
- [diagnose ipv6 devconf on page 311](#)
- [diagnose ipv6 ipv6-tunnel on page 312](#)
- [diagnose ipv6 neighbor-cache on page 312](#)
- [diagnose ipv6 route on page 313](#)
- [diagnose ipv6 sit-tunnel on page 314](#)
- [diagnose log alertconsole on page 314](#)
- [diagnose loop-guard status on page 316](#)
- [diagnose option82-mapping relay on page 317](#)
- [diagnose option82-mapping snooping on page 317](#)
- [diagnose settings on page 317](#)
- [diagnose sniffer packet on page 318](#)
- [diagnose snmp on page 320](#)
- [diagnose stp instance list on page 320](#)
- [diagnose stp mst-config list on page 322](#)
- [diagnose stp rapid-pvst-port on page 323](#)
- [diagnose stp vlan list on page 323](#)
- [diagnose switch 802-1x status on page 325](#)
- [diagnose switch 802-1x status-dacl on page 326](#)
- [diagnose switch acl counter on page 326](#)
- [diagnose switch acl hw-entry-index on page 328](#)
- [diagnose switch acl schedule on page 328](#)
- [diagnose switch arp-inspection stats clear on page 329](#)
- [diagnose switch cpuq on page 329](#)
- [diagnose switch egress list on page 330](#)
- [diagnose switch fortalink-auth statistics on page 331](#)
- [diagnose switch fortalink-auth status on page 331](#)
- [diagnose switch hsr on page 331](#)
- [diagnose switch ip-mac-binding entry on page 331](#)
- [diagnose switch ip-source-guard hardware entry filter on page 332](#)
- [diagnose switch ip-source-guard hardware entry list on page 332](#)
- [diagnose switch mac-address on page 333](#)
- [diagnose switch macsec statistics on page 334](#)
- [diagnose switch macsec status on page 335](#)

- [diagnose switch managed-switch on page 335](#)
- [diagnose switch mclag on page 335](#)
- [diagnose switch mirror auto-config on page 336](#)
- [diagnose switch mirror hardware status on page 337](#)
- [diagnose switch modules on page 338](#)
- [diagnose switch mrp on page 339](#)
- [diagnose switch network-monitor on page 339](#)
- [diagnose switch pdu-counters on page 340](#)
- [diagnose switch physical-ports cable-diag on page 341](#)
- [diagnose switch physical-ports datarate on page 342](#)
- [diagnose switch physical-ports eee-status on page 342](#)
- [diagnose switch physical-ports hw-counter on page 343](#)
- [diagnose switch physical-ports io-stats on page 344](#)
- [diagnose switch physical-ports led-flash on page 345](#)
- [diagnose switch physical-ports linerate on page 345](#)
- [diagnose switch physical-ports list on page 345](#)
- [diagnose switch physical-ports list on page 345](#)
- [diagnose switch physical-ports mdix-status on page 347](#)
- [diagnose switch physical-ports port-stats on page 347](#)
- [diagnose switch physical-ports qos-rates on page 348](#)
- [diagnose switch physical-ports qos-stats on page 350](#)
- [diagnose switch physical-ports list on page 345](#)
- [diagnose switch physical-ports set-counter-revert on page 351](#)
- [diagnose switch physical-ports list on page 345](#)
- [diagnose switch physical-ports list on page 345](#)
- [diagnose switch physical-ports list on page 345](#)
- [diagnose switch physical-ports summary on page 353](#)
- [diagnose switch physical-ports cable-diag on page 341](#)
- [diagnose switch poe status on page 354](#)
- [diagnose switch prp on page 355](#)
- [diagnose switch cpuq on page 329](#)
- [diagnose switch ptp port get-link-delay on page 355](#)
- [diagnose switch qnq dtag-cfg on page 356](#)
- [diagnose switch storm-control on page 356](#)
- [diagnose switch trunk list on page 357](#)
- [diagnose switch trunk summary on page 359](#)
- [diagnose switch vlan on page 360](#)
- [diagnose switch vlan-mapping egress hardware-entry on page 362](#)
- [diagnose switch vlan-mapping ingress hardware-entry on page 362](#)
- [diagnose switch vxlan arp-nd-cache on page 362](#)
- [diagnose switch vxlan mac-address list on page 363](#)
- [diagnose switch vxlan vp-info on page 363](#)
- [diagnose sys checkused on page 363](#)
- [diagnose sys cpuset on page 364](#)
- [diagnose sys dayst-info on page 364](#)

- [diagnose sys fan status on page 364](#)
- [diagnose sys fan-cloud-mgr on page 365](#)
- [diagnose sys flash on page 365](#)
- [diagnose sys flow-export on page 366](#)
- [diagnose sys kill on page 366](#)
- [diagnose sys link-monitor on page 366](#)
- [diagnose sys mpstat on page 367](#)
- [diagnose sys ntp status on page 367](#)
- [diagnose sys pcb temp on page 367](#)
- [diagnose sys permission list on page 368](#)
- [diagnose sys permission list-by-accprofile on page 368](#)
- [diagnose sys permission list-cli on page 369](#)
- [diagnose sys process on page 369](#)
- [diagnose sys psu status on page 370](#)
- [diagnose sys remote assistance on page 370](#)
- [diagnose sys sniffer-profile on page 371](#)
- [diagnose sys soc temp on page 371](#)
- [diagnose sys top on page 372](#)
- [diagnose sys vlan list on page 373](#)
- [diagnose test application on page 373](#)
- [diagnose test authserver on page 374](#)
- [diagnose user radius coa on page 375](#)

## diagnose automation test

Use this command to test the specified automation stitch:

```
diagnose automation test <automation-stitch-name> [<log_ID>]
```

### Example output

```
S224ENTF18000826 # diagnose automation test teststitch 0  
automation test is done. stitch:teststitch
```

## 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 116](#).

## 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 certificate all

Use this command to verify all system certificates:

```
diagnose certificate all
```

## Example output

```
S148EN5919002268 # diagnose certificate all
```

```
Certificate Authority
```

```
-----
```

```
Name : Fortinet_802.1x_CA
Fingerprint(MD5) : AA:EE:5C:F8:B0:D8:59:6D:2E:0C:BE:67:42:1C:F7:DB
Serial Number : 04:e1:e7:a4:dc:5c:f2:f3:6d:c0:2b:42:b8:5d:15:9f
Integrity : Passed
Timeliness : Valid (Expires on 2028-10-22 12:00:00 GMT)
```

```
Name : Fortinet_CA
Fingerprint(MD5) : 86:40:5C:F4:C2:A6:0B:96:82:9E:5F:E7:4F:D9:51:22
Serial Number : 00
Integrity : Passed
Timeliness : Valid (Expires on 2056-05-27 20:27:39 GMT)
```

```
Name : Fortinet_CA2
Fingerprint(MD5) : 85:A9:7C:FC:85:D6:2D:8B:9F:18:0A:8B:50:29:04:A9
Serial Number : da:f6:36:b4:43:d4:a5:8b
Integrity : Passed
Timeliness : Valid (Expires on 2038-01-19 22:34:39 GMT)
```

```
Name : Fortinet_Sub_CA2
Fingerprint(MD5) : 2E:36:70:82:7F:1E:21:CE:94:20:82:01:62:5E:30:DD
Serial Number : 20:01
Integrity : Passed
Timeliness : Valid (Expires on 2056-05-27 20:48:33 GMT)
```

```
Name : Fortinet_fsw_cloud_CA
Fingerprint(MD5) : AA:EE:5C:F8:B0:D8:59:6D:2E:0C:BE:67:42:1C:F7:DB
Serial Number : 04:e1:e7:a4:dc:5c:f2:f3:6d:c0:2b:42:b8:5d:15:9f
Integrity : Passed
Timeliness : Valid (Expires on 2028-10-22 12:00:00 GMT)
```

#### Local

---

```
Name : Fortinet_802.1x
Fingerprint(MD5) : 0C:7B:E2:32:85:D0:05:DA:CA:16:15:86:82:D7:28:63
Serial Number : 0d:b1:1b:bc:13:51:13:23:18:64:23:55:cd:db:3b:fe
Integrity : Passed
Key-pair : Passed
Timeliness : Valid (Expires on 2022-05-24 12:00:00 GMT)
```

```
Name : Fortinet_Factory
Fingerprint(MD5) : A0:20:10:10:17:D5:13:E5:9D:93:72:F4:FB:37:10:57
Serial Number : 0e:98:f9
Integrity : Passed
Key-pair : Passed
Timeliness : Valid (Expires on 2056-01-19 03:14:07 GMT)
```

```
Name : Fortinet_Factory2
Fingerprint(MD5) : 3B:73:EC:E9:6E:F1:39:12:32:16:A5:16:79:E4:04:0C
Serial Number : 4b:6e:10
Integrity : Passed
Key-pair : Passed
```

```

Timeliness      : Valid (Expires on 2038-01-19 03:14:07 GMT)

Name            : Fortinet_Firmware
Fingerprint(MD5) : A3:09:DB:D7:31:CA:7C:A6:CD:03:B1:91:FB:D7:13:23
Serial Number   : 41:1d:d5
Integrity       : Passed
Key-pair        : Passed
Timeliness      : Valid (Expires on 2038-01-19 03:14:07 GMT)

Remote
-----

```

## diagnose certificate ca

Use this command to verify CA certificates:

```
diagnose certificate ca
```

### Example output

```

S148EN5919002268 # diagnose certificate ca

Name            : Fortinet_802.1x_CA
Fingerprint(MD5) : AA:EE:5C:F8:B0:D8:59:6D:2E:0C:BE:67:42:1C:F7:DB
Serial Number   : 04:e1:e7:a4:dc:5c:f2:f3:6d:c0:2b:42:b8:5d:15:9f
Integrity       : Passed
Timeliness      : Valid (Expires on 2028-10-22 12:00:00 GMT)

Name            : Fortinet_CA
Fingerprint(MD5) : 86:40:5C:F4:C2:A6:0B:96:82:9E:5F:E7:4F:D9:51:22
Serial Number   : 00
Integrity       : Passed
Timeliness      : Valid (Expires on 2056-05-27 20:27:39 GMT)

Name            : Fortinet_CA2
Fingerprint(MD5) : 85:A9:7C:FC:85:D6:2D:8B:9F:18:0A:8B:50:29:04:A9
Serial Number   : da:f6:36:b4:43:d4:a5:8b
Integrity       : Passed
Timeliness      : Valid (Expires on 2038-01-19 22:34:39 GMT)

Name            : Fortinet_Sub_CA2
Fingerprint(MD5) : 2E:36:70:82:7F:1E:21:CE:94:20:82:01:62:5E:30:DD
Serial Number   : 20:01
Integrity       : Passed
Timeliness      : Valid (Expires on 2056-05-27 20:48:33 GMT)

Name            : Fortinet_fsw_cloud_CA
Fingerprint(MD5) : AA:EE:5C:F8:B0:D8:59:6D:2E:0C:BE:67:42:1C:F7:DB

```

```
Serial Number   : 04:e1:e7:a4:dc:5c:f2:f3:6d:c0:2b:42:b8:5d:15:9f
Integrity       : Passed
Timeliness      : Valid (Expires on 2028-10-22 12:00:00 GMT)
```

## diagnose certificate local

Use this command to verify local certificates:

```
diagnose certificate local
```

### Example output

```
S548DF5018000776 # diagnose certificate local

Name           : Fortinet_802.1x
Fingerprint(MD5) : 0C:7B:E2:32:85:D0:05:DA:CA:16:15:86:82:D7:28:63
Serial Number   : 0d:b1:1b:bc:13:51:13:23:18:64:23:55:cd:db:3b:fe
Integrity       : Passed
Key-pair        : Passed
Timeliness      : Valid (Expires on 2022-05-24 12:00:00 GMT)

Name           : Fortinet_Factory
Fingerprint(MD5) : B1:92:9D:7B:63:4B:9D:F7:57:FF:E6:59:AE:C2:21:2A
Serial Number   : 19:c1:ea
Integrity       : Passed
Key-pair        : Passed
Timeliness      : Valid (Expires on 2038-01-19 03:14:07 GMT)

Name           : Fortinet_Factory2
Fingerprint(MD5) : F8:E4:51:61:B6:F0:98:FA:43:1F:4C:FD:C1:5D:B2:62
Serial Number   : 19:c1:ec
Integrity       : Passed
Key-pair        : Passed
Timeliness      : Valid (Expires on 2038-01-19 03:14:07 GMT)

Name           : Fortinet_Firmware
Fingerprint(MD5) : A3:09:DB:D7:31:CA:7C:A6:CD:03:B1:91:FB:D7:13:23
Serial Number   : 41:1d:d5
Integrity       : Passed
Key-pair        : Passed
Timeliness      : Valid (Expires on 2038-01-19 03:14:07 GMT)
```

## diagnose certificate remote

Use this command to verify remote certificates:

```
diagnose certificate remote
```

## 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 debugging level is returned.

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

The following applications are supported:

- alerterd—Monitor and alert daemon
- authd—Authentication control daemon
- auto-script—Automation script
- autod—Automation stitch
- bfdd—Bidirectional forwarding detection (BFD) daemon
- bgpd—Border Gateway Protocol (BGP) daemon
- ctrlld—General FortiSwitch control daemon
- cu\_swtpd—Switch-controller CAPWAP control daemon
- dhcp6c—DHCPv6 client module
- dhcpc—DHCP client module
- dhcprelay—DHCP relay daemon
- dmid—Diagnostic monitoring interface (DMI) daemon
- dnsproxy—DNS proxy module
- eap\_proxy—EAP proxy daemon
- email-server—Email server
- erspan-auto-mgr—ERSPAN-auto mode configuration resolution daemon
- flcmdd—FortiLink command daemon
- flow-export—Flow-export
- fnbamd—FortiGate nonblocking authentication daemon
- fortilinkd—FortiLink daemon
- fpm—Hardware routing daemon
- flannmgr—FortiLAN Cloud daemon
- gratarp—IP conflict gratuitous ARP utility
- gui—GUI service
- httpsd—HTTP and HTTPS daemon
- ip6addrd—IPv6 address utility
- ipconflictd—IP conflict detection daemon
- isisd—Intermediate System to Intermediate System Protocol (IS-IS) daemon
- l2d—Daemon for layer-2 features
- l2dbg—Daemon for hardware-related operations needed by layer 2
- l3—Layer-3 debugging
- lacpd—Link Aggregation Control Protocol (LACP) daemon

- libswitchd—FortiSwitch library daemon
- link-monitor—Link monitor daemon
- lldpmedd—Link Layer Discovery Protocol-Media Endpoint Discovery (LLPD-MED) daemon
- mcast-snooping—Multicast-snooping debugging
- miglogd—Logging daemon
- mrpd—Media Redundancy Protocol (MRP) daemon
- ntpd—Network Time Protocol (NTP) daemon
- nwmcfgd—Daemon for network-monitoring configuration
- nwmonitord—Packet-handling and parsing daemon for network monitoring
- ospf6d—Open shortest path first (OSPF IPv6) routing daemon
- ospfd—Open shortest path first (OSPF IPv4) routing daemon
- pbrd—Policy-based routing (PBR) daemon
- pimd—Protocol Independent Multicast (PIM) daemon
- portspeedd—Port speed daemon
- radius\_das—RADIUS CoA daemon
- radiusd—RADIUS daemon
- radvd—Router advertisement daemon
- ripd—Routing Information Protocol (RIP) routing daemon
- ripngd—Routing Information Protocol NG (RIPNG) daemon
- router-launcher—Daemon for launching the routing system
- rsyslogd—Remote SYSLOG daemon
- sflowd—sFlow daemon
- snmpd—Simple Network Management Protocol (SNMP) daemon
- sshd—Secure Sockets Shell (SSH) daemon
- staticd—Static route daemon
- statsd—Statistics collection daemon
- stpd—Spanning Tree Protocol (STP) daemon
- switch-launcher—Daemon for launching the FortiSwitch system
- trunkd—Trunk daemon
- vrrpd—Virtual Router Redundancy Protocol (VRRP) daemon
- vxland—Virtual Extensible LAN (VXLAN) daemon.
- wiredap—Daemon for 802.1x port-based authentication
- wpa\_supp—MACsec Key Agreement (MKA) MACsec daemon
- 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 fssso clear-logons
diagnose debug authd fssso filter clear
diagnose debug authd fssso filter group <group_name>
diagnose debug authd fssso filter server <FSSO_agent_name>
diagnose debug authd fssso filter source <IPv4_address> <IPv4_address>
diagnose debug authd fssso filter user <user_name>
diagnose debug authd fssso list
diagnose debug authd fssso refresh-groups
diagnose debug authd fssso refresh-logons
diagnose debug authd fssso server-status
diagnose debug authd fssso summary
```

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

### Example output

```
diag debug authd fssso server-status
```

```
Server Name      Connection Status      Version
-----
fssso            connected               FSSO 5.0.0237
```

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

## diagnose debug bfd

Use this command to enable, show, or disable the debugging level for bidirectional forwarding detection (BFD):

```
diagnose debug bfd {all | appl | fsm | net | show | zebra } {enable | disable}
```

## diagnose debug bgp

Use this command to enable, show, or disable the debugging level for Border Gateway Protocol (BGP) routing:

```
diagnose debug bgp {all | appl | as4 | flowspec | keepalives | neighbor-events | nht | normal | show
| updates | zebra} {enable | disable}
```

## 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.

Variable	Description
fssso	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 | kill-with-crashlog <process_ID> | read}
```

Variable	Description
clear	Clear the crash log.
get	Display the crash log on the console.
kill-with-crashlog <process_ID>	End the daemon using the specified process ID.
read	Display the crash log on the console in a readable format.

### Example output

```
S524DF4K15000024 # diagnose debug crashlog get

Rk9SVP94nDK0NLPUNTSNTZUMDSzMjCwMjVXSEr0jc9IzEvJSY3PTM8tKI5Pzk2x
UvB1dGw00Q1xdPJx1Q32jHK1MjQwMuECCCAjA0NzXQNLXQMzBU0gZgMrQ0uFkoxU
hezMnJzUFIWUxNTc/DyFzGIF/aTMPP301JKSSiuF4pLEktJiW4MKAy6AAELWb2gF
dIKJKUn6AQIIVb+JmZWpCUn6AQIIVb+RlYGx1bExSfoBAghZv7GVqamVEWn+Bwgg
ZP0mVgYWwCAkST9AAKHqNzQHxR8p+gECCFW/MdALhiToN+ICCCA0/WZwxqTpBwgg
```

```
ZP3AwDMGJKGS3A8QQKj6TYBJwIIk/QABhKbfBBiFJLkFIIDQ9JtaGZNivxEXQAAh
6zcDxb8RafEHEECo+oH+NyAt/QMEEKp+UP41Ikk/QADB9ZuD8r+RpRXQIOL1GxsY
cAEEEKoJphakpgCAAELWbwgKQQPSQhAggFD1A30AMWkhABBAaPotrUxIsx8ggJD1
A0sgU1JzMEAAIesHZ18jICJJp0AAIesHpgBz0koAAy6AAELWb24FTgQk6QcIIFT9
JkD3k5KCDLgAAghNPzD+SbMfIIBQ9ZsaAyshkvQDBBCyfQDlwEKYtBIIIBQ9Q0j
0IS08AcIIDT9ZqS1HyMugABC1W8EDH/SakCAAELVD8w/JMY/QAAh6wcWH0bAJECS
foAAguu3UDAwtzIClmCk1B+gEggggJBNSLQCV8MkuQAggND0A+sA01IQQACH6jC
1mGk1YAAAAYSkH1gCGZkCnUCSfoAAQtUPKGFJsx8ggFD1mwBzEGklGEAAoek3AUyi
...
```

```
S548DF5018000776 # diagnose debug crashlog read
```

```
1: 2020-03-13 11:54:15 the killed daemon is /bin/fsmgrd: status=0x0
2: 2020-03-13 16:55:27 the killed daemon is /bin/fsmgrd: status=0x0
3: 2020-03-13 16:59:09 the killed daemon is /bin/fsmgrd: status=0x0
4: 2020-03-13 17:32:56 the killed daemon is /bin/fsmgrd: status=0x0
5: 2020-03-13 18:10:52 the killed daemon is /bin/fsmgrd: status=0x0
6: 2020-03-13 18:45:45 the killed daemon is /bin/fsmgrd: status=0x0
7: 2020-03-13 18:52:24 the killed daemon is /bin/fsmgrd: status=0x0
8: 2020-03-16 11:59:48 restart_reason=SYSTEM SHUTDOWN
9: 2020-03-17 10:16:42 restart_reason=SYSTEM SHUTDOWN
10: 2020-03-23 09:23:22 restart_reason=SYSTEM SHUTDOWN
11: 2020-03-24 08:33:04 restart_reason=SYSTEM SHUTDOWN
12: 2020-03-26 08:11:33 restart_reason=SYSTEM SHUTDOWN
13: 2020-04-10 08:48:25 restart_reason=SYSTEM SHUTDOWN
14: 2020-05-06 10:51:28 the killed daemon is /bin/fsmgrd: status=0x0
15: 2020-05-06 11:47:45 the killed daemon is /bin/fsmgrd: status=0x0
16: 2020-05-06 17:49:04 the killed daemon is /bin/fsmgrd: status=0x0
17: 2020-05-28 08:45:54 restart_reason=SYSTEM SHUTDOWN
18: 2020-05-28 09:09:00 the killed daemon is /bin/fsmgrd: status=0x0
19: 2020-05-28 09:36:23 the killed daemon is /bin/fsmgrd: status=0x0
20: 2020-05-28 18:12:20 the killed daemon is /bin/fsmgrd: status=0x0
21: 2020-05-29 13:31:52 the killed daemon is /bin/fsmgrd: status=0x0
22: 2020-05-29 15:04:20 the killed daemon is /bin/fsmgrd: status=0x0
23: 2020-05-29 16:01:28 the killed daemon is /bin/fsmgrd: status=0x0
24: 2020-05-29 16:27:41 the killed daemon is /bin/fsmgrd: status=0x0
25: 2020-06-01 16:04:11 restart_reason=SYSTEM SHUTDOWN
26: 2020-06-02 09:56:49 the killed daemon is /bin/fsmgrd: status=0x0
```

## 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 isis

Use this command to enable, show, or disable the debugging level for Intermediate System to Intermediate System Protocol (IS-IS) routing:

```
diagnose debug isis {adj-packets | all | appl | bfd | events | flooding | lsp-gen | lsp-sched |
  packet-dump | route-events | show | snp-packets | spf-events | tx-queue | update-packets}
  {enable | disable}
```

## 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 ospf

Use this command to enable, show, or disable the debugging level for open shortest path first (OSPF) routing for IPv4 traffic:

```
diagnose debug ospf {all | appl | event | ism-debug | lsa-debug | nsm-debug | nssa | packet-debug |  
show | zebra-debug} {enable | disable}
```

## diagnose debug ospf6

Use this command to enable or disable the debugging level for open shortest path first (OSPF) routing for IPv6 traffic:

```
diagnose debug ospf6 {abr | all | appl | asbr | border-routers | flooding | interface | lsa | lsa-  
debug | message | neighbor | packet-debug | route | route-debug | spf | zebra} {enable |  
disable}
```

## 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 pbr

Use this command to enable, show, or disable the debugging level for policy-based routing (PBR):

```
diagnose debug pbr {all | appl | events | map | nht | show | zebra} {enable | disable}
```

## diagnose debug pim

Use this command to enable, show, or disable the debugging level for Protocol Independent Multicast (PIM) routing:

```
diagnose debug pim {all | appl | events | igmp-events | igmp-packets | igmp-trace | mroute | packet-  
dump | packets | show | static | trace | zebra} {enable | disable}
```

## diagnose debug port-mac

**NOTE:** This command is available only on FortiSwitch units that have the split-port feature available.

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 debug rip

Use this command to enable, show, or disable the debugging level for IPv4 Routing Information Protocol (RIP) routing:

```
diagnose debug rip {all | appl | events | packet-rx | packet-tx | show | zebra} {enable | disable}
```

## diagnose debug ripng

Use this command to enable, show, or disable the debugging level for IPv6 Routing Information Protocol (RIP) routing:

```
diagnose debug ripng {all | appl | events | packet-rx | packet-tx | show | zebra} {enable | disable}
```

## diagnose debug static

Use this command to enable or disable the debugging level for static routes:

```
diagnose debug static {all | appl} {enable | disable}
```

## diagnose debug unit\_test

Use this command to enable or disable the debugging of unit tests:

```
diagnose debug unit_test {enable | disable}
```

### Example output

```
S524DF4K15000024 # diagnose debug unit_test enable
libsw_unit_test argc 2
cmd =0
```

## diagnose debug zebra

Use this command to enable, show, or disable the debugging level for the core router daemon:

```
diagnose debug zebra {all | appl | events | fpm | kernel | packet-rx | packet-rx-detail | packet-tx
| packet-tx-detail | rib | rib-queue | show} {enable | disable}
```

## diagnose firewall ip clear-counter

Use this command to clear the IPv4 iptables counter:

```
diagnose firewall ip clear-counter
```

## diagnose firewall ip show

Use this command to show IPv4 iptables:

```
diagnose firewall ip show
```

## diagnose firewall ipv6 clear-counter

Use this command to clear the IPv6 iptables counter:

```
diagnose firewall ipv6 clear-counter
```

## diagnose firewall ipv6 show

Use this command to show IPv6 iptables:

```
diagnose firewall ipv6 show
```

## diagnose flapguard status

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

```
diagnose flapguard status
```

### Example output

```
S524DF4K15000024 # diagnose flapguard status
```

Portname	State	Status	Timeout(m)	flap-rate	flap-duration	
flaps/duration	Last-Event					
port1	disabled	-	-	5	30	0
-						
port2	disabled	-	-	5	30	0
-						
port3	disabled	-	-	5	30	0
-						

port4	disabled	-	-	5	30	0
-						
port5	disabled	-	-	5	30	0
-						
port6	disabled	-	-	5	30	0
-						
port7	disabled	-	-	5	30	0
-						
port8	disabled	-	-	5	30	0
-						
port9	enabled	-	0	5	30	0
-						
port10	disabled	-	-	5	30	0
-						
port11	disabled	-	-	5	30	0
-						
port12	disabled	-	-	5	30	0
-						
port13	disabled	-	-	5	30	0
-						
port14	disabled	-	-	5	30	0
-						
port15	disabled	-	-	5	30	0
-						
port16	disabled	-	-	5	30	0
-						
port17	disabled	-	-	5	30	0
-						
port18	disabled	-	-	5	30	0
-						
port19	enabled	-	30	15	10	0
-						
port20	disabled	-	-	5	30	0
-						
port21	disabled	-	-	5	30	0
-						
port22	disabled	-	-	5	30	0
-						
port23	disabled	-	-	5	30	0
-						
port24	disabled	-	-	5	30	0
-						
port25	disabled	-	-	5	30	0
-						
port26	disabled	-	-	5	30	0
-						
port27	disabled	-	-	5	30	0
-						

port28	disabled	-	-	5	30	0
-						
port29	disabled	-	-	5	30	0
-						
port30.1	disabled	-	-	5	30	0
-						
port30.2	disabled	-	-	5	30	0
-						
port30.3	disabled	-	-	5	30	0
-						
port30.4	disabled	-	-	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 ioport {byte <value> | long <arguments> | word <arguments>}
diagnose hardware switchinfo {l2-station-table | l3-ecmp-table | l3-egress-table | l3-host-table |
    l3-intf-table | l3-ip-mapping-table | l3-pbr-mapping-table | l3-pbr-nhop-group-table | l3-
    routing-table | l3-summary | l3-v6-host-table | l3-v6-routing-table | multicast-groups}
diagnose hardware sysinfo {bootenv | cpu | interrupts | iomem | memory | slab}
diagnose hardware usb
```

Variable	Description
certificate	Verify which certificates are present on the FortiSwitch unit and that all installed certificates are valid.
ioport {byte <value>   long <arguments>   word <arguments>}	Read and write data using the input/output port.
{l2-station-table   l3-ecmp-table   l3-egress-table   l3-host-table   l3-intf-table   l3-ip-mapping-table   l3-pbr-mapping-table   l3-pbr-nhop-group-table   l3-routing-table   l3-summary   l3-v6-host-table   l3-v6-routing-table   multicast-groups}	Display information about the FortiSwitch hardware.
sysinfo {bootenv   cpu   interrupts   iomem   memory   slab}	Display information about the system.
usb	Display information about the connected USB devices.

## Example output

```
S548DF5018000776 # diagnose hardware certificate
Checking Fortinet_CA.cer integrity .....Passed
Checking Fortinet_Factory.cer integrity .....Passed
Checking Fortinet_Factory.cer key-pair integrity .....Passed
Checking Fortinet_Factory.cer Serial-No. ....Passed
Checking Fortinet_Factory.cer timeliness .....Passed
Checking Fortinet_Factory.key integrity .....Passed
Checking Fortinet_CA2.cer integrity .....Passed
Checking Fortinet_Factory2.cer integrity .....Passed
Checking Fortinet_Factory2.cer key-pair integrity .....Passed
Checking Fortinet_Factory2.cer Serial-No. ....Passed
Checking Fortinet_Factory2.cer timeliness .....Passed
Checking Fortinet_Factory2.key integrity .....Passed
```

```
S524DF4K15000024 # diagnose hardware switchinfo l3-ip-mapping-table
Ip Addr          Intf  EgressObj  Mac          Static-ARP    VRF
111.222.1.1      39   100005    00:00:00:00:00:00  0              0
```

```
S524DF4K15000024 # diagnose hardware switchinfo l3-egress-table
L3 Egress entries: Max: 16384 Existing 6
Entry  Mac          Vlan INTF  PORT  MOD  MPLS_LABEL  ToCpu Drop RefCount L3MC
100002 00:00:00:00:00:00 4095  0    0    0    -1  yes  no    1  no
100003 00:00:00:00:00:00 4092  1    0    0    -1  yes  no    1  no
100004 00:00:00:00:00:00 4094  2    0    0    -1  yes  no    1  no
100005 04:d5:90:97:e1:16 4094  2    0t   0    -1  no   no    1  no
100006 00:00:00:00:00:00  10   3    0    0    -1  yes  no    1  no
```

```
S424EPTF19000004 # diagnose hardware usb
Alea II TRNG
EHCI Host Controller
Generic Platform OHCI controller
```

```
FS1E483Z17000008 # diagnose hardware switchinfo l2-station-table
Priority  Mac          Vlan  SrcPort  Flags
0        70:4c:a5:53:ca:a8 4095  0x8000001 0x1c
0        70:4c:a5:53:ca:d2 4095  0x800002b 0x1c
0        70:4c:a5:53:ca:ce 4095  0xc000000 0x1c
0        70:4c:a5:53:ca:ae 4095  0x8000007 0x1c
0        70:4c:a5:53:ca:cc 4095  0x8000025 0x1c
0        70:4c:a5:53:ca:be 4095  0x8000017 0x1c
```

```
FS1E483Z17000008 # diagnose hardware switchinfo multicast-groups
```

```
Group 0x1000000 (L2)
```

```
port ge0, encap -1
port xe0, encap -1
port ge1, encap -1
port ge2, encap -1
port xe1, encap -1
port xe2, encap -1
port ge3, encap -1
port xe3, encap -1
port xe4, encap -1
port xe5, encap -1
port xe6, encap -1
port xe7, encap -1
port xe8, encap -1
port xe9, encap -1
port ge4, encap -1
port xe10, encap -1
port xe11, encap -1
port xe12, encap -1
port xe13, encap -1
port xe14, encap -1
port xe15, encap -1
port xe16, encap -1
port ge5, encap -1
port xe17, encap -1
port ge6, encap -1
port xe18, encap -1
port xe19, encap -1
port xe20, encap -1
port xe21, encap -1
port xe22, encap -1
port xe23, encap -1
port xe24, encap -1
port xe25, encap -1
port xe26, encap -1
port xe27, encap -1
port xe28, encap -1
port ge7, encap -1
port xe29, encap -1
port ge8, encap -1
port ge9, encap -1
port xe30, encap -1
port xe31, encap -1
port ge10, encap -1
port xe32, encap -1
port xe33, encap -1
port xe34, encap -1
port xe35, encap -1
port xe36, encap -1
port ce0, encap -1
port ce1, encap -1
```

```

    port ce2, encap -1
    port ce3, encap -1

Group 0x7000002 (VLAN)
    port cpu0, encap -1

Group 0x2000003 (L3)
    port ge0, encap -1
    port ge3, encap -1
    port ge5, encap -1
    port ge7, encap -1
    port ge8, encap -1
    port ge9, encap -1
    port ge10, encap -1

```

## 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

```
S524DF4K1500024 # diagnose ip arp list

index=2 ifname=mgmt 10.105.16.1 90:6c:ac:15:2f:94 state=00000002 use=117606 confirm=537
update=67371 ref=1
index=70 ifname=internal 192.168.0.10 state=00000001 use=24 confirm=178601 update=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.

Variable	Description
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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=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 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->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 pref=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 pref=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 pref=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 pref=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 pref=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 pref=192.168.1.99
gwy=0.0.0.0 dev=2(mgmt)

```

## diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra}

Use these commands to display statistics for bidirectional forwarding detection (BFD), Border Gateway Protocol (BGP) routing, Intermediate System to Intermediate System Protocol (IS-IS) routing, open shortest path first (OSPF) routing for IPv4 traffic, OSPF routing for IPv6 traffic, Protocol Independent Multicast (PIM) routing, policy-based routing (PBR), Routing Information Protocol (RIP) routing for IPv4 traffic, RIP routing for IPv6 traffic, static routes, and core routing daemon:

```

diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra} cpu-
usage
diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra}
crash-backtrace-clear
diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra}
crash-backtrace-read
diagnose ip router zebra fpm-counters clear
diagnose ip router zebra fpm-counters show
diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra}
memory-usage
diagnose ip router {bfd | bgp | isis | ospf | ospf6 | pim | pbr | rip | ripng | static | zebra}
work-queues

```

Variable	Description
cpu-usage	Display statistics for CPU usage.
crash-backtrace-clear	Delete the crash-backtrace information.
crash-backtrace-read	Display the crash-backtrace information.
fpm-counters clear	Erase the hardware offload counters.
fpm-counters show	Display the hardware offload counters.
memory-usage	Display statistics for memory usage.
work-queues	Display information about work queues.

## diagnose ip router command

Use these commands to send commands to various daemons in enable mode (cmd) or in configure terminal mode (cmd-conf-term):

```
diagnose ip router command bfd {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command bgp {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command isis {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command ospf {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command ospf6 {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command pim {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command rip {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command static {cmd <arguments>| cmd-conf-term <arguments>}
diagnose ip router command zebra {cmd <arguments>| cmd-conf-term <arguments>}
```

## diagnose ip router fwd

Use these commands for debugging layer-3 forwarding:

```
diagnose ip router fwd l3-clear-stats
diagnose ip router fwd l3-disable-ip-tracing
diagnose ip router fwd l3-ecmp
diagnose ip router fwd l3-egress
diagnose ip router fwd l3-enable-ip-tracing <IP_address>
diagnose ip router fwd l3-enable-ip-tracing6 <IPv6_address>
diagnose ip router fwd l3-intf
diagnose ip router fwd l3-rvi-dev-info <RVI_name>
diagnose ip router fwd l3-rvi-info
diagnose ip router fwd l3-stats
```

Variable	Description
l3-clear-stats	Delete layer-3 statistics.

Variable	Description
l3-disable-ip-tracing	Disable IP tracing.
l3-ecmp	Display information about equal cost multi-path (ECMP) routing.
l3-egress	Display layer-3 egress information.
l3-enable-ip-tracing <IP_address>	Enable IPv4 host tracing
l3-enable-ip-tracing6 <IPv6_address>	Enable IPv6 host tracing.
l3-intf	Display information about layer-3 interfaces.
l3-rvi-dev-info <RVI_name>	Display RVI internal information.
l3-rvi-info	Display which ports and trunks are RVIs.
l3-stats	Display layer-3 statistics.

## Example

```
FS1E483Z17000008 # diagnose ip router fwd l3-rvi-dev-info RVI10
RVI trunkid: -1: Ifindex: 64 Numlinks: 0 port: 1
(Port,StationId): (1,1)
```

```
FS1E483Z17000008 # diagnose ip router fwd l3-rvi-info
RVI port1: Ifindex: 64
RVI port7: Ifindex: 67
RVI port23: Ifindex: 73
RVI port37: Ifindex: 69
RVI port39: Ifindex: 77
RVI port40: Ifindex: 77
RVI port43: Ifindex: 74
RVI trunk0: Ifindex: 77
Port Info: port1 port7 port23 port37 port39 port40 port43 internal
```

## diagnose ip router process show

Use this command to display information about the process launch of the core routing daemon, static routing daemon, BGD daemon, OSPF (IPv4 and IPv6) daemons, BFD daemon, RIP daemon, IS-IS daemon, and PIM daemon:

```
diagnose ip router process show
```

## 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 rtcache list

Use this command to list the routing cache:

```
diagnose ip rtcache list
```

## diagnose ip rules list

Use this command to list IP rules.

```
diagnose ip rules list
```

### Example

```
S524DF4K15000024 # diagnose ip rules list
tab=0 fam=2 action=1 flags: 0x0 prio=1000 src=0.0.0.0/0 dst=0.0.0.0/0 table=(0)
tab=0 fam=2 action=7 flags: 0x0 prio=2000 src=0.0.0.0/0 dst=0.0.0.0/0 table=(0)
tab=255 fam=2 action=1 flags: 0x0 prio=32765 src=0.0.0.0/0 dst=0.0.0.0/0 table=(255)
tab=254 fam=2 action=1 flags: 0x0 prio=32766 src=0.0.0.0/0 dst=0.0.0.0/0 table=(254)
tab=253 fam=2 action=1 flags: 0x0 prio=32767 src=0.0.0.0/0 dst=0.0.0.0/0 table=(253)
```

## 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

```

S524DF4K1500024 # 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.

Variable	Description
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 preferred=-1 valid=-1
dev=2 devname=mgmt flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fe1:95e4 preferred=-1 valid=-1
dev=70 devname=internal flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fe1:95e5 preferred=-1
valid=-1
dev=71 devname=vlan35 flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fe1:95e5 preferred=-1 valid=-1
dev=72 devname=vlan85 flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fe1:95e5 preferred=-1 valid=-1
dev=74 devname=vlan-8 flag=P scope=253 prefix=64 addr=fe80::a5b:eff:fe1:95e5 preferred=-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: <ul style="list-style-type: none"> <li>0 – disable duplicate address detection.</li> <li>1 – enable duplicate address detection.</li> <li>2 – enable duplicate address detection and disable IPv6 operation if duplicate MAC-based link-local addresses are found.</li> </ul>
disable_ipv6 {0   1 }	Configure IPv6 operation: <ul style="list-style-type: none"> <li>0 – enable IPv6 operation.</li> <li>1 – disable IPv6 operation.</li> </ul>

## 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> <IPv6_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 confirm=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=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.
fgd-retrieve	Retrieve FortiGuard alert console messages.
list	List current alert console messages.
test	Generate alert console messages.



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

## diagnose loop-guard status

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

```
diagnose loop-guard status
```

To enable loop guard on a port, see [config switch interface on page 116](#).

### Example output

```
S524DF4K15000024 # diagnose loop-guard status
```

Portname	State	Status	Timeout(m)	MAC-Move	Count	Last-Event
port1	disabled	-	-	-	-	-
port2	disabled	-	-	-	-	-
port3	disabled	-	-	-	-	-
port4	disabled	-	-	-	-	-
port5	disabled	-	-	-	-	-
port6	disabled	-	-	-	-	-
port7	disabled	-	-	-	-	-
port10	disabled	-	-	-	-	-
port11	disabled	-	-	-	-	-
port12	enabled	-	45	0	0	-
port13	disabled	-	-	-	-	-
port14	disabled	-	-	-	-	-
port15	disabled	-	-	-	-	-
port16	disabled	-	-	-	-	-
port17	disabled	-	-	-	-	-
port18	disabled	-	-	-	-	-
port19	disabled	-	-	-	-	-
port20	disabled	-	-	-	-	-
port21	enabled	-	45	50	0	-
port22	disabled	-	-	-	-	-
port24	disabled	-	-	-	-	-
port25	disabled	-	-	-	-	-
port26	disabled	-	-	-	-	-
port27	disabled	-	-	-	-	-
port28	disabled	-	-	-	-	-
port29	disabled	-	-	-	-	-
port30.1	disabled	-	-	-	-	-
port30.2	disabled	-	-	-	-	-

```
port30.3      disabled - - - -  
port30.4      disabled - - - -  
G100D3G15817028 disabled - - - -
```

## diagnose option82-mapping relay

Use this command to display the option-82 setting for DHCP relay for each valid system interface:

```
diagnose option82-mapping relay <valid_system_interface>
```

### Example output

```
S524DF4K15000024 # diagnose option82-mapping relay internal
```

```
Interface Name Remote-ID(hex) Circuit-ID(hex)  
internal 085B0EF195E5 00000000
```

## diagnose option82-mapping snooping

Use this command to display the option-82 settings for DHCP snooping for a specific VLAN and FortiSwitch interface:

```
diagnose option82-mapping snooping <VLAN_ID> <valid_switch_interface>
```

### Example output

```
S524DF4K15000024 # diagnose option82-mapping snooping 100 port2
```

```
Interface Name Remote-ID(hex) Circuit-ID(hex)  
port2 085B0EF195E5 00640102
```

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

Variable	Description
	diagnose sniffer packet internal "(ether [0:4]=0x00090f89) and (ether[4:2]=0x10ea)"
<verbose   1-6>	Set the level of detail for the results: <ul style="list-style-type: none"> <li>• verbose – Display all details.</li> <li>• 1 – Include the packet header.</li> <li>• 2 – Include the packet header and IP address data.</li> <li>• 3 – Include the packet header and Ethernet address data (if available).</li> <li>• 4 – Include the packet header and interface name.</li> <li>• 5 – Include the packet header, interface name, and IP address data.</li> <li>• 6 – Include the packet header, interface name, and Ethernet address data (if available).</li> </ul>
<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

```
S524DF4K1500024 # 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
...

S524DF4K1500024 # 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 167](#).

Variable	Description
<STP_ID>	Enter the STP identifier. If you enter a higher number than the valid range, the results for all STP instances are displayed. If no STP identifier is specified, 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 0
```

```
MST Instance Information, primary-Channel:
```

```
Instance ID 0 (CST)
```

```
Config      Priority 32768
             Bridge MAC 085b0ef195e4, MD5 Digest 40d5eca178c657835c83bbcb16723192
```

```
Root        MAC 085b0ef195e4, Priority 32768, Path Cost 0, Remaining Hops 20
             (This bridge is the root)
```

```
Regional Root MAC 085b0ef195e4, Priority 32768, Path Cost 0
             (This bridge is the regional root)
```

```
Active Times Forward Time 15, Max Age 20, Remaining Hops 20
```

```
TCN Events   Triggered 1 (1d 0h 19m 56s ago), Received 0 (1d 0h 19m 56s ago)
```

Port	Speed	Cost	Priority	Role	State	HelloTime	Flags
port1	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port3	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port4	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port5	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port6	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port7	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port8	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port9	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port10	-	200000000	128	DISABLED	DISCARDING	2	EN ED
port11	-	200000000	128	DISABLED	DISCARDING	2	EN ED

```

port12      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port13      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port14      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port17      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port18      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port19      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port20      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port21      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port22      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port23      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port24      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port25      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port26      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port27      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port28      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port29      -      200000000 128      DISABLED  DISCARDING  2      EN ED
port30      -      200000000 128      DISABLED  DISCARDING  2      EN ED
internal    1G      20000      128      DESIGNATED  FORWARDING  2      ED
Mclag-icl-trunk -      200000000 128      DISABLED  DISCARDING  2      ED
first-mclag -      200000000 128      DISABLED  DISCARDING  2      EN ED

```

Flags: EN(STP enable), ED(Edge), LP(Loop Protection), RG(Root Guard Triggered), BG(BPDU Guard Triggered)

## 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 169](#).

### 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 rapid-pvst-port

Use these commands to diagnose the interoperability with per-VLAN RSTP (Rapid PVST+ or RPVST+):

```
diagnose stp rapid-pvst-port clear [<port_name>]
diagnose stp rapid-pvst-port list [<port_name>]
```

Variable	Description
clear [<port_name>]	Clear all flags and timers on the RPVST+ port.
list [<port_name>]	Show the status of one port or all ports. If any of the ports is in the "IC" state, the command output gives the reason: VLAN priority inconsistent, VLAN configuration mismatch, or both.

## 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 Loop Protection	Speed	Cost	Priority	Role	State	Edge	STP-Status
port1 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port2 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port3 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port4 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port5 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port6 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port9 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port10 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port11 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port12 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port13 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port14 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port15 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port16 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port17 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port18 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port19 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port20 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port21 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED

port22 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port23 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port24 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port25 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port26 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port27 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port28 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port29 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
port30 NO	-	200000000	128	DISABLED	DISCARDING	YES	ENABLED
internal NO	1G	20000	128	DESIGNATED	FORWARDING	YES	DISABLED

## 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. In the output, the value in the “Traffic-Vlan” column is the VLAN where the client was successfully authenticated.

To enable IEEE 802.1x authentication on a port, see [config switch interface on page 116](#).

### Example output

```
S548DF4K15000195 # diagnose switch 802-1x status

port3 : Mode: mac-based (mac-by-pass disable)
Link: Link up
Port State: authorized: ( )
EAP pass-through : Enable
EAP auto-untagged-vlans : Disable
```

```

Quarantine VLAN (4093) detection : Enable
Native Vlan : 10
Allowed Vlan list: 10,15
Untagged Vlan list: 10
Guest VLAN :
Auth-Fail Vlan :

Switch sessions 2/240, Local port sessions:2/20
Client MAC Type           Traffic-Vlan      Dynamic-Vlan
94:10:3e:b9:12:65 802.1x          10             0
cc:5a:53:5f:d5:16 802.1x          10             15

```

## Sessions info:

```

94:10:3e:b9:12:65 Type=802.1x,TLS,state=AUTHENTICATED,etime=0,eap_cnt=8 params:reAuth=3600
cc:5a:53:5f:d5:16 Type=802.1x,TLS,state=AUTHENTICATED,etime=0,eap_cnt=7 params:reAuth=3600

```

## diagnose switch 802-1x status-dacl

Use this command to display the status of dynamic access control lists (DACLs) on 802.1x ports:

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

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

### Example output

```

S148FNTF20000098 # diagnose switch 802-1x status-dacl port11

port11: Mode: port-based (mac-by-pass disable)
DACL :enable: :

```

## 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 acl hw-entry-index

**NOTE:** This command is available only for the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.

Use this command to find the hardware mapping for the specified ACL policy identifier:

```
diagnose switch acl hw-entry-index <id>
```

Variable	Description
<id>	Enter the ACL policy identifier.

### Example output

```
S124EP4N17000016 # diagnose switch acl hw-entry-index 1
ID HW-INDEX AGG CNTR-IDX
-----
000001 896 n 7
```

## diagnose switch acl schedule

Use this command to list ACL policies with a schedule:

```
diagnose switch acl schedule egress
diagnose switch acl schedule ingress
diagnose switch acl schedule prelookup
```

Variable	Description
egress	List all ACL egress policies with a schedule.
ingress	List all ACL ingress policies with a schedule.
prelookup	List all ACL prelookup policies with a schedule.

### Example output

```
S524DF4K15000024 # diagnose switch acl schedule ingress
ACL Ingress Name
1      In Schedule
```

## 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 174](#).

## diagnose switch cpuq

### NOTES:

- Be careful about changing the CPU queue rate because the change is made directly to the hardware.
- After the switch is rebooted, the CPU queue rate returns to the default value.
- For the FS-108E and FS-124E families, the configured CPU queue rate has a 16-kbps granularity. Use the `diagnose switch cpuq show` command to see the actual queue rate.
- For the FS-108E and FS-124E families, the CPU queue rate is more accurate with larger packets.

To display the CPU queue rate on the FSR-112D-POE, FSR-216F-POE, FS-1xxE, FS-2xx, FS-4xx, FS-5xx, FS-1xxx, and FS-3xxx families:

```
diagnose switch cpuq show
```

To change the CPU queue rate on the FSR-112D-POE, FSR-216F-POE, FS-2xx, FS-4xx, FS-5xx, FS-1xxx, and FS-3xxx families:

```
diagnose switch cpuq rate <queue_number> <new_pps_rate>
```

To change the CPU queue rate on the FS-108E and FS-124E families:

```
diagnose switch cpuq rate <queue_number> <new_Kbps_rate>
```

Variable	Description
show	Display the CPU queue rate for all queues.
rate <queue_number> <new_pps_rate>	Change the CPU queue rate for the specified queue to the new packets-per-second (PPS) rate.
diagnose switch cpuq rate <queue_number> <new_Kbps_rate>	Change the CPU queue rate for the specified queue to the new Kbps rate.

## Example output (FS-548)

**NOTE:** The number of queues, queue classifications, and default CPU queue rates can differ among the FortiSwitch platforms.

```
S548DF5018000776 # diagnose switch cpuq show
Queue | Rate(pps)
-----
17     2000    (MIRROR/SFLOW)
18     500     (L3_DEST_MISS)
19     5000    (ARP_REQ)
20     10000   (DEFAULT)
21     1000    (NHOP)
22     8000    (DHCP/OSPF/BFD/RIP/IGMP/FORTLINK_VLAN)
23     6000    (ARP_REPLY)
24     5000    (FORTILINK/MCLAG)
25     1500    (BPDU/LOOPGUARD)
```

## 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 fortilink-auth statistics

Use this command to get the FortiLink authentication traffic statistics for the port from the FortiSwitch unit:

```
diagnose switch fortilink-auth statistics <port_name>
```

## diagnose switch fortilink-auth status

Use this command to get the FortiLink authentication status for the port from the FortiSwitch unit:

```
diagnose switch fortilink-auth status <port_name>
```

## diagnose switch hsr

Use these commands to troubleshoot your HSR configuration.

```
diagnose switch hsr {clear | config | node-table | settings | stats | status | vdan-table}
```

Variable	Description
clear	Delete the HSR statistics from the FortiSwitch unit.
config	Display the current HSR configuration.
node-table	Display the HSR node table.
settings	Display the current HSR settings.
stats	Display the HSR statistics.
status	Display the current HSR status.
vdan-table	Display the HSR virtual doubly attached node (VDAN) table.

## 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 105](#).

## 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 ip-source-guard hardware entry filter

Use these commands to select which IP source-guard entries to display:

```
diagnose switch ip-source-guard hardware entry filter clear
diagnose switch ip-source-guard hardware entry filter interface <interface_name>
diagnose switch ip-source-guard hardware entry filter ip <IPv4_address>
diagnose switch ip-source-guard hardware entry filter mac <MAC_address>
diagnose switch ip-source-guard hardware entry filter print
```

Variable	Description
clear	Remove the current filter.
interface <port_name>	Display entries for the specified port.
ip <IPv4_address>	Display entries for the specified IPv4 address.
mac <MAC_address> <mask>	Delete entries for the specified MAC address and mask.
print	Display the current filter.

## diagnose switch ip-source-guard hardware entry list

Use this command to display all IP source-guard entries. Static entries were manually added by the `config switch ip-source-guard` command. Dynamic entries were added by DHCP snooping.

```
diagnose switch ip-source-guard hardware entry list
```

## 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.
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 commas. For example: 1,2-4,77
list	List the MAC address entries and the total number of 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 list
```

```
MAC: 08:5b:0e:f1:95:e5  VLAN: 4094 Port: internal(port-id 31)
Flags: 0x00010460 [ static hit src-hit native ]
```

```
MAC: d6:dd:25:be:2c:43 VLAN: 1 Port: port1(port-id 1)
Flags: 0x00000020 [ static ]

Total Displayed: 2

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 macsec statistics

Use this command to display MACsec traffic statistics for the specified port. If no port is specified, statistics for all ports are returned.

```
diagnose switch macsec statistics [<port_name>]
```

## diagnose switch macsec status

Use this command to display the MACsec status of the specified port. If no port is specified, the status for all ports is returned.

```
diagnose switch macsec status [<port_name>]
```

## diagnose switch managed-switch

Use these commands to display information about the FortiSwitch unit when it is managed by a FortiGate unit:

```
diagnose switch managed-switch dump xlate-vlan
diagnose switch managed-switch dump trunk
```

## diagnose switch mclag

Use these commands to manage information about multichassis link aggregation groups (MCLAGs):

```
diagnose switch mclag clear-stats all
diagnose switch mclag clear-stats icl
diagnose switch mclag clear-stats mclag <trunk_name>
diagnose switch mclag icl
diagnose switch mclag list <trunk_name>
diagnose switch mclag peer-consistency-check
diagnose switch mclag peer-consistency-check <MCLAG_trunk_name>
diagnose switch mclag peer-consistency-check help
```

Variable	Description
clear-stats all	Delete the statistics for all MCLAGs.
clear-stats icl	Delete the statistics for the MCLAG ICLs.
clear-stats mclag <MCLAG_trunk_name>	Delete the statistics for the specified MCLAG trunk.
icl	List all inter-chassis links (ICLs).
list <trunk_name>	Display statistics for the MCLAG with the specified trunk.
peer-consistency-check	Check all local MCLAGs or MCLAG-ICL-enabled link aggregation groups (LAGs).
peer-consistency-check <MCLAG_trunk_name>	Check the specified MCLAG or MCLAG-ICL-enabled link aggregation group (LAG).
peer-consistency-check help	Provide more information about the diagnose switch mclag peer-consistency-check options.

To set up an MCLAG, see [config switch trunk on page 170](#).

## Example output

```
Switch1 # diagnose switch mclag icl
ICL-trunk
  icl-ports 47-48
  egress-block-ports 3,37
  interface-mac 08:5b:0e:73:fb:e7
  local-serial-number FS1D483Z14000113
  peer-mac 08:5b:0e:73:f8:87
  peer-serial-number FS1D483Z14000097
  Local uptime 0 days 3h:57m:59s
  Peer uptime 0 days 3h:57m:16s
  MCLAG-STP-mac 08:5b:0e:73:f8:86
  keepalive interval 1
  keepalive timeout 60
  dormant candidate Peer
  split-brain Normal

Counters
  received keepalive packets 14012
  transmitted keepalive packets 14012
  received keepalive drop packets 2
```

## diagnose switch mirror auto-config

Use these commands to manage switch mirroring using ERSPAN encapsulation with automatically configured header contents:

```
diagnose switch mirror auto-config restart
diagnose switch mirror auto-config status
```

Variable	Description
restart	Restart the ERSPAN mirroring daemon.
status	Display the status of the ERSPAN mirroring.

## Example output

```
S524DF4K15000024 # diagnose switch mirror auto-config status
Session name:
Last update: never
Error msg:
State: None
Flags: 0x00000000 ()
```

```
Config:
  Last good config update: never

Route Lookup:
  Last good route update: never
  Collector IP: 0.0.0.0
  Nexthop IP: 0.0.0.0
  SVI name:
  SVI devindex: 0
  SVI source MAC: 00:00:00:00:00:00
  SVI VLAN: 0
  SVI source IP: 0.0.0.0

Nexthop ARP resolution:
  Last good ARP update: never
  Nexthop MAC: 00:00:00:00:00:00

Switching table resolution:
  Last good update: never
  L2 result: MAC: 00:00:00:00:00:00 VLAN: 0
              port-id: 0 Flags: 0x00000000
  Switch interface:
  Switch interface VLAN 0: untagged

Hardware updates:
  Last good update: never
  Last failed update: never
  Last update return: 0:Success.

Resolved/Running state:
  Last entered: never
  Last left: never
```

## diagnose switch mirror hardware status

Use this command to display information about the driver-level and hardware-level switch mirroring:

```
diagnose switch mirror hardware status
```

### Example output

```
S524DF4K15000024 # diagnose switch mirror hardware status

[flink.sniffer]=====
  Installed           : no ( inactive)
```

# 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
-----|-----
port | curr state | prev state | -IC | DMI | Module | Type | State | Temp | Vcc | TxBia | TxPwr | RxPwr |
-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
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 | .. | .. | .. | .. | .. | .. | .. | .. |
```



Variable	Description
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

```
S548DN5018000377 # diagnose switch pdu-counters list
primary CPU counters:
packet receive error : 0
Non-zero port counters:
port1:
    IGMP Membership Report : 45
    IGMP Membership Leave : 3
    IGMPv3 Membership Report : 69002
port13:
    IGMP Query packet : 50794
    IGMPv3 Membership Report : 50794
port47:
    LACP packet : 15474
    STP packet : 237919
    LLDP packet : 168194
    IGMP Query packet : 50757
    IGMP Membership Report : 29
    IGMP Membership Leave : 1
port48:
    LACP packet : 15475
    STP packet : 6
    LLDP packet : 168192
port51:
    IGMP Membership Report : 19
    IGMP Membership Leave : 4
    IGMPv3 Membership Report : 4
```

## diagnose switch physical-ports cable-diag

Use this command to display the results of a time-domain reflectometer (TDR) diagnostic test on the specified port.

```
diagnose switch physical-ports cable-diag <port_name>
```

## 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
```

## diagnose switch physical-ports datarate

Use this command to 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.

```
diagnose switch physical-ports datarate [<port_list>]
```

### Example output

```
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
```

## diagnose switch physical-ports eee-status

Use this command to display whether the specified port has energy-efficient Ethernet (EEE) enabled. If the port is not specified, the status of all ports is displayed.

```
diagnose switch physical-ports eee-status [<port_name>]
```

### Example output

```
S524DF4K15000024 # diagnose switch physical-ports eee-status port9
Portname  State    RX-LPI-Status TX-LPI-Status TX(ms) RX(ms) TX-Resolved(ms) RX-Resolved(ms)
-----|-----|-----|-----|-----|-----|-----|-----|
port9     Enabled Inactive  Inactive      0         0         0             0
```

## diagnose switch physical-ports hw-counter

Use these commands to display information about counters:

```
diagnose switch physical-ports hw-counter add {rx | tx} <counter_id> <counter|counter|counter...>
diagnose switch physical-ports hw-counter clear {rx | tx} <counter_id>
diagnose switch physical-ports hw-counter info
diagnose switch physical-ports hw-counter remove {rx | tx} <counter_id> <counter|counter|counter...>
diagnose switch physical-ports hw-counter search <port_name> <interval_seconds>
    <counter|counter|counter...>
diagnose switch physical-ports hw-counter search-cancel
diagnose switch physical-ports hw-counter search-results
diagnose switch physical-ports hw-counter show {rx | tx | all} <port_name>
```

Variable	Description
hw-counter add {rx   tx} <counter_id> <counter counter counter...>	Add trigger flags to a specified counter.
hw-counter clear {rx   tx} <counter_id>	Clear a specific counter.
hw-counter info	Display the supported trigger flags (RX and TX).
hw-counter remove {rx   tx} <counter_id> <counter counter counter...>	Remove trigger flags from the specified counters.
hw-counter search <port_name> <interval_seconds> <counter counter counter...>	Retrieve the data for the specified triggers on a specified port within the interval in seconds.
hw-counter search-cancel	Cancel the currently running search.
hw-counter search-results	Display the last search results.
hw-counter show {rx   tx   all} <port_name>	Show all trigger flags and statistics on a specified port.

### Example output

```
S524DF4K1500024 # diagnose switch physical-ports hw-counter show all port9
```

```
-----
|                               Counter Statistics (port:9)                               |
-----
|Type|Counter ID|      Value      |      Trigger Flags Enabled      |
-----
| Rx |           0 |                | 0|RIPD4 RIPD6 RDISC RPORTD PDISC |
|   |           |                | | RFILDR RDROP VLANDR           |
-----
| Rx |           1 |                | 0|IMBP                            |
```

```

-----
| Rx |      2 |          0|RIMDR
-----
| Tx |      0 |          0|TGIP6 TGIPMC6
-----
| Tx |      1 |          0|TIPD6 TIPMCD6
-----
| Tx |      2 |          0|TGIPMC6
-----
| Tx |      3 |          0|TPKTD
-----
| Tx |      4 |          0|TGIP4 TGIP6
-----
| Tx |      5 |          0|TIPMCD4 TIPMCD6
-----
| Tx |      6 |          0|THIGIG2
-----

```

## diagnose switch physical-ports io-stats

Use these commands to display information about input/output packet statistics:

```

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>]

```

Variable	Description
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.

### Example output

```

S524DF4K15000024 # diagnose switch physical-ports io-stats cumulative
Cumulative IO Stats:
RX PacketsBpdu          69035
RX PacketsL3RxCpu      1020
RX PacketsRxAll        112157
RX PacketsFlpOrIGMP    39831
-----

```

## diagnose switch physical-ports led-flash

Use this command to flash all port LEDs on and off for a specified number of minutes so that a particular switch can be identified. Valid times are 5, 15, 30, or 60 minutes. Use `disable` to stop the LEDs from flashing.

```
diagnose switch physical-ports led-flash disable
diagnose switch physical-ports led-flash {5 | 15 | 30 | 60}
```

## diagnose switch physical-ports linerate

Use this command to 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.

```
diagnose switch physical-ports linerate [<port_list>]
```

### Example output

```
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
```

## diagnose switch physical-ports list

Use this command to display the details for the specified port. If the port is not specified, the details for all ports are displayed.

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

### Example output

```
S524DF4K15000024 # diagnose switch physical-ports list port1
```

```

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

```

## diagnose switch physical-ports mapping

Use this command to display which drivers are associated with which ports:

```
diagnose switch physical-ports mapping
```

### Example output

```

S524DF4K15000024 # diagnose switch physical-ports mapping
Unmapped port IDs:
Userspace      |
Port Name      | PortID | Driver
-----|-----|-----
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
```

## diagnose switch physical-ports mdix-status

Use this command to display whether a specified port is a medium-dependent interface crossover (MDIX) port:

```
diagnose switch physical-ports mdix-status <port_name>
```

### Example output

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

## diagnose switch physical-ports port-stats

Use these commands to list port statistics for the specified ports or list port statistics that are not zero. Use commas to separate ports. If the ports are not specified, the statistics for all ports are displayed.

```
diagnose switch physical-ports port-stats [<port_list> | non-zero]
```

### Example output

```
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 Octets Packets: 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
```

---

## diagnose switch physical-ports qos-rates

Use these commands to display real-time egress QoS queue rates, including the data rate, line rate, and drop rate:

```
diagnose switch physical-ports qos-rates clear <port_list>
```

```
diagnose switch physical-ports qos-rates list [<port_list>]
diagnose switch physical-ports qos-rates non-zero
```

Variable	Description
qos-rates clear <port_list>	Delete the QoS statistics for the specified ports. If the ports are not specified, the statistics for all ports are deleted.
qos-rates list [<port_list>]	Display the real-time egress QoS queue rates for the specified ports. If the ports are not specified, the rates for all ports are displayed. Press Ctrl+c to stop the output.
qos-stats non-zero	Display only the real-time egress QoS queue rates that are not zero. Press Ctrl+c to stop the output.

## Example output

```
S548DF5018000776 # diagnose switch physical-ports qos-rates non-zero
```

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

```
ctrl-c to
port6 QoS Rates:
```

queue	PPS	data(Mbps)	line(Mbps)	drop (PPS)	drop(Mbps)
7	0.0000	0.0000	0.0000	0.0000	0.0000

```
port28 QoS Rates:
```

queue	PPS	data(Mbps)	line(Mbps)	drop (PPS)	drop(Mbps)
7	0.8466	0.0008	0.0010	0.0000	0.0000

```
internal QoS Rates:
```

queue	PPS	data(Mbps)	line(Mbps)	drop (PPS)	drop(Mbps)
25	0.8472	0.0009	0.0010	0.0000	0.0000

```
ctrl-c to stop
^C
```

## diagnose switch physical-ports qos-stats

Use these commands to display QoS statistics:

```
diagnose switch physical-ports qos-stats clear <port_list>
diagnose switch physical-ports qos-stats list [<port_list>]
diagnose switch physical-ports qos-stats non-zero
diagnose switch physical-ports qos-stats set-qos-counter-revert [<port_list>]
diagnose switch physical-ports qos-stats set-qos-counter-zero [<port_list>]
```

Variable	Description
qos-stats clear [<port_list>]	Delete the QoS statistics for the specified ports. If the ports are not specified, the statistics for all ports are deleted.
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.
qos-stats non-zero	List only QoS statistics that are not zero.
qos-stats set-qos-counter-revert [<port_list>]	Restore QoS counters to direct hardware values for the specified ports. Use commas to separate ports. If the ports are not specified, the command affects all ports.
qos-stats set-qos-counter-zero [<port_list>]	Clear QoS counters (applies to all applications except SNMP) for the specified ports. Use commas to separate ports. If the ports are not specified, the command affects all ports.

### Example output

```
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
-----

```

## diagnose switch physical-ports queue-bandwidth-setting

Use these commands to display the bandwidth setting (kbps or percentage) for the egress queues. If the ports are not specified, the bandwidth setting for all egress queues are displayed.

```
diagnose switch physical-ports queue-bandwidth-setting [<port_list>]
```

### Example output

```
S524DF4K15000024 # diagnose switch physical-ports queue-bandwidth-setting port23
```

```
port23 cosq bandwidth setting: (0: disabled)
```

port	q	KbpsMin	KbpsMax
port23	0	0	0
port23	1	0	0
port23	2	0	0
port23	3	0	0
port23	4	0	0
port23	5	0	0
port23	6	0	0
port23	7	0	0

## diagnose switch physical-ports set-counter-revert

Use this command to restore hardware counters (except for QoS, SNMP, and web GUI counters) on the specified ports. Use commas to separate ports. If the ports are not specified, the command affects all ports.

```
diagnose switch physical-ports set-counter-revert [<port_list>]
```

## diagnose switch physical-ports set-counter-zero

Use this command to clear all hardware counters (except for QoS, SNMP, and web GUI counters) on the specified ports. Use commas to separate ports. If the ports are not specified, the command affects all ports.

```
diagnose switch physical-ports set-counter-zero [<port_list>]
```

## diagnose switch physical-ports split-status

Use this command to display information about split ports:

```
diagnose switch physical-ports split-status
```

### Example output

```
S524DF4K15000024 # diagnose switch physical-ports split-status
Port Name          Split Phy Name      Port Index    Child Index
-----
port29             No -                29            -
port30.1           Yes port30             30            0
port30.2           Yes port30             32            1
port30.3           Yes port30             33            2
port30.4           Yes port30             34            3
```

## diagnose switch physical-ports stats

Use these commands to display counter statistics:

```
diagnose switch physical-ports stats clear-local <port_list>
```

```
diagnose switch physical-ports stats list [<port_list>]
```

```
diagnose switch physical-ports stats non-zero
```

Variable	Description
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.
stats non-zero	List the statistics for counters that are not zero.

## Example output

```
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 |
```

## diagnose switch physical-ports summary

Use this command to display a summary about the specified physical port. If the port is not specified, summaries for all ports are displayed.

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

## Example output

```
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)
```

## diagnose switch physical-ports virtual-wire list

Use this command to list all virtual wires:

```
diagnose switch physical-ports virtual-wire list
```

## Example output

```
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 <physical_port_name>
```

Variable	Description
<physical_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 prp

Use these commands to troubleshoot your PRP configuration:

```
diagnose switch prp {clear | config | node-table | settings | stats | status | vdan-table}
```

Variable	Description
clear	Delete the PRP statistics from the FortiSwitch unit.
config	Display the current PRP configuration.
node-table	Display the PRP node table.
settings	Display the current PRP settings.
stats	Display the PRP statistics.
status	Display the current PRP status.
vdan-table	Display the PRP VDAN table.

## diagnose switch ptp port add-link-delay

Use this command to add an estimated link delay in nanoseconds to the specified port. Adding a link delay helps with debugging, and the setting is cleared when the switch is rebooted:

```
diagnose switch ptp port add-link-delay <port_name> <estimated_link_delay>
```

### Example output

```
S548DN4K15000008 # diagnose switch ptp port add-link-delay port49 500
Adding port49's link_delay 500(ns).
```

## diagnose switch ptp port get-link-delay

Use this command to display link-delay information for the specified port:

```
diagnose switch ptp port get-link-delay <port_name>
```

## Example output

```
S548DN4K15000008 # diagnose switch ptp port get-link-delay port49
```

Portname	Speed	Link-Delay
port49	10G	500ns

## diagnose switch qnq dtag-cfg

Use this command to display information about the VLAN stacking (QinQ) configuration:

```
diagnose switch qnq dtag-cfg
```

## Example output

```
S548DF5018000776 # diagnose switch qnq dtag-cfg
```

Port Name	QinQ Mode	Add Inner-Tag	Remove Inner-Tag	Priority	Ether-Type
port39	customer	add (vid 456)	enable	follow-s-tag	0x8100

## diagnose switch storm-control

Use this command to display the storm-control configuration and the current drop rate:

```
diagnose switch storm-control
```

## Example output on FS-448E

```
S448ENTF20000009 # diagnose switch storm-control
```

```
storm-control-monitor  enabled
high-rate              600pps
rate-filter            80%
port                  rate
-----
port1                  0
port2                  141
port3                  0
.
```

```

.
.

```

## Example output on FS-124E

```

S124EN4N17002007 # diagnose switch storm-control

storm-control-monitor  enabled

port      storm control drop
-----
port1
port2      unicast, broadcast
port3
.
.
.

```

## 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

S524DF4K15000024 # diagnose switch trunk list

Switch Trunk Information, primary-Channel

Trunk Name: Mclag-icl-trunk
Mode: lacp-active (mclag-icl)
Port Selection Algorithm: N/A - Trunk Down
Trunk MAC: 08:5B:0E:F1:95:F4

Active Port  Up  Time
-----
Non-Active Port  Status
-----

port15          BLOCK
port16          BLOCK

LACP flags: (A|P)(S|F)(A|I)(I|O)(E|D)(E|D)
(A|P) - LACP mode is Active or Passive
(S|F) - LACP speed is Slow or Fast
(A|I) - Aggregatable or Individual
(I|O) - Port In sync or Out of sync
(E|D) - Frame collection is Enabled or Disabled
(E|D) - Frame distribution is Enabled or Disabled

status: down
ports: 2
LACP mode: active
LACP speed: slow
aggregator ID: 1
actor key: 0
actor MAC address: 08:5b:0e:f1:95:f4
partner key: 1
partner MAC address: 00:00:00:00:00:00

slave: port15
status: down
link failure count: 0
permanent MAC addr: 08:5b:0e:f1:95:f4
actor state: ASAIDD
partner state: PSIODD
aggregator ID: 1

slave: port16
status: down
link failure count: 0
permanent MAC addr: 08:5b:0e:f1:95:f5
actor state: ASAODD

```

```

partner state: PSIODD
aggregator ID: 2

Trunk Name:  first-mclag
Mode:  static (mclag)
Port Selection Algorithm:  N/A - Trunk Down
Trunk MAC:  08:5B:0E:F1:95:E7

Active Port  Up  Time
-----
Non-Active Port  Status
-----
port2           BLOCK

```

## diagnose switch trunk summary

Use this command to display a summary of the link aggregation information:

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

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

### Example output

```

S524DF4K15000024 # diagnose switch trunk summary

Trunk Name      Mode                PSC      MAC                Status      Up
Time
-----
Mclag-icl-trunk lACP-active(mclag-icl) N/A      08:5B:0E:F1:95:F4 down(0/2)
N/A
first-mclag     static(mclag)       N/A      08:5B:0E:F1:95:E7 down(0/1)
N/A
8DN3X16000001-0 lACP-active(auto-isl) src-dst-ip 08:5B:0E:F0:9B:90 up(1/1)    0
days,0 hours,1 mins,35 secs

S524DF4K15000024 # diagnose switch trunk summary first-mclag

```

Trunk Name Time	Mode	PSC	MAC	Status	Up
first-mclag N/A	static(mclag)	N/A	08:5B:0E:F1:95:E7	down(0/1)	

## 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 cache <VLAN_ID>
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.

Variable	Description
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 cache <VLAN_ID>	Display information about the VLAN cache.
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

```
S524DF4K1500024 # 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

S524DF4K1500024 # 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 switch vlan-mapping egress hardware-entry

Use the following command to check the VLAN mapping on an interface for the egress direction:

```
diagnose switch vlan-mapping egress hardware-entry
```

## diagnose switch vlan-mapping ingress hardware-entry

Use the following command to check the VLAN mapping on an interface for the ingress direction:

```
diagnose switch vlan-mapping ingress hardware-entry
```

## diagnose switch vxlan arp-nd-cache

Use the following commands to clear or display the Address Resolution Protocol (ARP)/Neighbor Discovery (ND) cache in the software for the local VXLAN hosts:

```
diagnose switch vxlan arp-nd-cache clear-stats <VLAN_ID>
diagnose switch vxlan arp-nd-cache show [<VLAN_ID>]
```

## diagnose switch vxlan mac-address list

Use the following command to list the MAC address, VXLAN network identifier (VNI), source and destination IP addresses of the VXLAN tunnel, and the VXLAN destination port for the specified VXLAN interface:

```
diagnose switch vxlan mac-address list <VXLAN_interface_name>
```

## diagnose switch vxlan vp-info

Use the following command to display information about virtual ports:

```
diagnose switch vxlan vp-info [<VLAN_ID>]
```

Variable	Description
[<VLAN_ID>]	Display information about the virtual ports for the specified VLAN. If the VLAN is not specified, the command displays information about all virtual ports.

## diagnose sys checkused

Use the following command 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

```
S524DF4K1500024 # 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-is1-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 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 flan-cloud-mgr

Use these commands to manage the SSL tunnel for FortiLAN Cloud management:

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

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

## 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
2 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 flow-export

Use these commands to manage flow-export data:

```
diagnose sys flow-export delete-flows-all
diagnose sys flow-export expire-flows-all
```

Variable	Description
delete-flows-all	Delete all flow-export data.
expire-flows-all	Expire all flow-export data.

## 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 373](#).

## 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 239](#).

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 244](#).

## 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 permission list

Use this command to list the permissions required to use the commands for the specified access profile groups:

```
diagnose sys permission list <all | <group_list>
```

Variable	Description
<group_list>	The access profile group can be any of the following: mntgrp, admingrp, swcoregrp, pktmongrp, sysgrp, netgrp, loggrp, routegrp, swmonguardgrp, utilgrp, utmgrp, or vmgrp. The permission level is r for read only or rw for read and write. For example, you can enter <code>diagnose sys permission list sysgrp:r+mntgrp:r+utilgrp:rw</code> .

## Example output

```
S224ENTF18000826 # diagnose sys permission list sysgrp:r
"diagnose certificate all" Read-permissions-required="sysgrp" Write-permissions-required="sysgrp"
"diagnose certificate ca" Read-permissions-required="sysgrp" Write-permissions-required="sysgrp"
"diagnose certificate local" Read-permissions-required="sysgrp" Write-permissions-
required="sysgrp"
"diagnose certificate remote" Read-permissions-required="sysgrp" Write-permissions-
required="sysgrp"
"diagnose switch managed-switch dump xlate-vlan" Read-permissions-required="sysgrp" Write-
permissions-required=""
"diagnose sys checkused" Read-permissions-required="sysgrp" Write-permissions-required=""
"diagnose sys ntp status" Read-permissions-required="sysgrp" Write-permissions-required=""...
```

## diagnose sys permission list-by-accprofile

Use this command to list the available commands and permissions for the specified access profile:

```
diagnose sys permission list-by-accprofile <access_profile_name>
```

Use the `get system accprofile` command to see the available access profiles.

## Example output

```
S224ENTF18000826 # diagnose sys permission list-by-accprofile prof_admin
"diagnose automation test" Read-permissions-required="loggrp" Write-permissions-required="loggrp"
"diagnose bpdu-guard status" Read-permissions-required="swmonguardgrp" Write-permissions-
required="swmonguardgrp"
"diagnose certificate all" Read-permissions-required="sysgrp" Write-permissions-required="sysgrp"
"diagnose certificate ca" Read-permissions-required="sysgrp" Write-permissions-required="sysgrp"
"diagnose certificate local" Read-permissions-required="sysgrp" Write-permissions-
required="sysgrp"
"diagnose certificate remote" Read-permissions-required="sysgrp" Write-permissions-
required="sysgrp"
"diagnose debug application alertd" Read-permissions-required="utilgrp" Write-permissions-
required="utilgrp"
"diagnose debug application authd" Read-permissions-required="utilgrp" Write-permissions-
required="utilgrp"
"diagnose debug application auto-script" Read-permissions-required="utilgrp" Write-permissions-
required="utilgrp"...
```

## diagnose sys permission list-cli

Use this command to list the permissions for the specified CLI path:

```
diagnose sys permission list-cli <CLI_path>
```

## Example output

```
S224ENTF18000826 # diagnose sys permission list-cli system.interface
"config system interface" Read-permissions-required="netgrp" Write-permissions-required="netgrp"
"get system interface physical" Read-permissions-required="netgrp" Write-permissions-
required="netgrp"
```

## 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 373](#).

## 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 remote assistance

After you have contacted Customer Support for assistance, Customer Support might ask you to open a remote assistance session. After you have entered one of the remote assistance commands, Customer Support can examine your FortiSwitch unit remotely to gather more data about your switch's configuration and to find the solution to the issue. The remote assistance session uses an SSL tunnel for a secure connection.

You can open a remote assistance session when your FortiSwitch unit is in standalone mode, in FortiLink mode, or managed by FortiLAN Cloud.

```
diagnose sys remote assistance disable
diagnose sys remote assistance indefinite
diagnose sys remote assistance limit <integer>
```

Variable	Description
disable	Disable the remote assistance session.
indefinite	Enable the remote assistance session until the FortiSwitch unit is rebooted or the <code>diagnose sys remote assistance disable</code> command is entered.
limit <integer>	Enable the remote assistance session for the specified number of hours. The range is 1-96 hours.

- Before opening a remote assistance session, your FortiSwitch unit must be able to connect to the Internet.
- Before requesting remote assistance, you must have registered your FortiSwitch unit with FortiCare Support Services (<https://www.fortinet.com/support-and-training/support-services/forticare-support.html>).
- If your FortiSwitch unit is managed by FortiLAN Cloud, opening a remote assistance session will end the connection between your FortiSwitch unit and FortiLAN Cloud.

## Example output

```
S524DF4K15000024 # diagnose sys remote assistance limit 1
Starting remote assistance ..... Complete.

S524DF4K15000024 # diagnose sys remote assistance indefinite
Starting remote assistance .... Complete.

S524DF4K15000024 # diagnose sys remote assistance disable
Stopping remote assistance session .... Complete.
```

## diagnose sys sniffer-profile

Use this command to display information about available packet-capture profiles:

```
diagnose sys sniffer-profile
```

### Example output

```
S224ENTF18000826 # diagnose sys sniffer-profile
Maximum Allowed Profile: 8.

Name          | Status   | Pkt-Count   | Profile-ID | Type      | PID
=====
NewPacketCapture | Stop    | 0           | 1          | SW-INTF  | 0
```

## diagnose sys soc temp

Use this command to display the temperature of the system-on-a-chip (SoC) die:

```
diagnose sys soc temp
```

### Example output

```
S224ENTF18000826 # diagnose sys soc temp

Module      Status
-----
Sensor1     47.3 C
```

## diagnose sys top

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

```
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 174](#).

## diagnose test application

Use these commands to test specific daemons:

```
diagnose test application dnspoxy <test_level>
diagnose test application fpm d <test_level>
diagnose test application radiusd <test_level>
diagnose test application sflowd <test_level>
diagnose test application snmpd <test_level>
```

Variable	Description
dnspoxy <test_level>	Specify the test level for the DNS proxy daemon: <ol style="list-style-type: none"> <li>1. Clear DNS cache.</li> <li>2. Show statistics.</li> <li>3. Dump DNS setting.</li> <li>4. Reload the fully qualified domain name (FQDN).</li> <li>5. Requery the FQDN.</li> <li>6. Dump the FQDN.</li> </ol>
fpm d <test_level>	Specify the test level for the hardware offload daemon.
radiusd <test_level>	Specify the test level for the RADIUS daemon: <ul style="list-style-type: none"> <li>• 2: Clear the RADIUS server database.</li> <li>• 3: Show the RADIUS server database.</li> <li>• 33: Show the RADIUS server database (with start time).</li> <li>• 4: Show the RADIUS server database information.</li> <li>• 9: Check the high availability (HA) context table checksums.</li> <li>• 11: Show the HA synchronization connection status.</li> <li>• 20: Show the RADIUS server configuration cache.</li> <li>• 21: Show the RADIUS server interface configuration cache.</li> <li>• 99: Restart.</li> </ul>
sflowd <test_level>	Specify the test level for the sFlow daemon: <ul style="list-style-type: none"> <li>• 1: Show collector setting.</li> <li>• 2: Show state.</li> </ul>

Variable	Description
snmpd <test_level>	Specify the test level for the SNMP daemon: <ul style="list-style-type: none"> <li>• 1: Display daemon process identifier.</li> <li>• 2: Display SNMP statistics.</li> <li>• 3: Clear SNMP statistics.</li> <li>• 4: Generate test trap.</li> <li>• 99: Restart daemon.</li> <li>• 101: Reset the msgAuthoritativeEngineBoots attribute to 0 and restart the daemon.</li> </ul>

## 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 fpm 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.

Variable	Description
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 270](#).

# execute

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

- [execute 802-1x clear mac on page 378](#)
- [execute 802-1x clear interface on page 378](#)
- [execute 802-1x dacl-clr-stat on page 379](#)
- [execute 802-1x dacl-reinstall on page 379](#)
- [execute acl clear-counter on page 379](#)
- [execute acl key-compaction on page 380](#)
- [execute alias configure on page 380](#)
- [execute alias script on page 382](#)
- [execute backup config on page 382](#)
- [execute acl key-compaction on page 380](#)
- [execute backup memory on page 384](#)
- [execute batch on page 385](#)
- [execute bpdu-guard on page 386](#)
- [execute cfg reload on page 387](#)
- [execute cfg save on page 387](#)
- [execute clear switch igmp-snooping on page 388](#)
- [execute clear switch mld-snooping on page 389](#)
- [execute clear system arp table on page 389](#)
- [execute cli check-template-status on page 390](#)
- [execute cli status-msg-only on page 390](#)
- [execute date on page 390](#)
- [execute dhcp lease-clear on page 391](#)
- [execute dhcp lease-list on page 391](#)
- [execute dhcp-snooping on page 392](#)
- [execute disconnect-admin-session on page 392](#)
- [execute factoryreset on page 393](#)
- [execute factoryresetfull on page 393](#)
- [execute flapguard reset on page 393](#)
- [execute fortilink-auth clearstat on page 394](#)
- [execute fortilink-auth reauth on page 394](#)
- [execute fortilink-auth reset on page 394](#)
- [execute interface dhcpclient-renew on page 394](#)
- [execute interface dhcp6client-renew on page 395](#)
- [execute interface pppoe-reconnect on page 395](#)
- [execute license add on page 395](#)
- [execute license enhanced-debugging on page 395](#)
- [execute license status on page 396](#)
- [execute log delete on page 396](#)
- [execute log delete-all on page 397](#)

- [execute log display on page 397](#)
- [execute log filter on page 397](#)
- [execute log-report reset on page 398](#)
- [execute loop-guard reset on page 399](#)
- [execute mac clear on page 399](#)
- [execute mac-limit-violation reset on page 399](#)
- [execute macsec clearstat physical-port on page 400](#)
- [execute macsec reset physical-port on page 400](#)
- [execute macsec toggle physical-port on page 401](#)
- [execute mtracroute on page 401](#)
- [execute ping on page 402](#)
- [execute ping-options on page 403](#)
- [execute ping6 on page 404](#)
- [execute ping6-options on page 405](#)
- [execute poe-reset on page 406](#)
- [execute reboot on page 407](#)
- [execute rest list on page 407](#)
- [execute rest login on page 408](#)
- [execute rest logout on page 408](#)
- [execute rest run on page 409](#)
- [execute rest schema on page 411](#)
- [execute restore bios on page 412](#)
- [execute restore config on page 412](#)
- [execute restore image on page 413](#)
- [execute restore license on page 414](#)
- [execute revision on page 415](#)
- [execute router clear bgp on page 416](#)
- [execute router clear evpn dup-addr on page 417](#)
- [execute router clear ospf on page 417](#)
- [execute router tech-support on page 417](#)
- [execute set-next-reboot on page 418](#)
- [execute shutdown on page 418](#)
- [execute source-guard-violation reset on page 419](#)
- [execute ssh on page 419](#)
- [execute on page 376](#)
- [execute stage on page 420](#)
- [execute sticky-mac on page 421](#)
- [execute switch-controller clear-nac-mac-cache on page 421](#)
- [execute switch-controller delete-nac-mac-cache on page 421](#)
- [execute switch-controller get-conn-status on page 422](#)
- [execute switch-controller get-nac-mac-cache on page 422](#)
- [execute system admin account-convert-sha1 on page 423](#)
- [execute system admin account-convert-sha256 on page 423](#)
- [execute system certificate crl import auto on page 424](#)
- [execute system certificate local export tftp on page 425](#)

- [execute system certificate local generate ec on page 425](#)
- [execute system certificate local generate rsa on page 426](#)
- [execute system certificate local import tftp on page 427](#)
- [execute system certificate remote on page 427](#)
- [execute system sniffer-profile delete-capture on page 428](#)
- [execute system sniffer-profile pause on page 428](#)
- [execute system sniffer-profile start on page 429](#)
- [execute system sniffer-profile stop on page 429](#)
- [execute system sniffer-profile upload on page 430](#)
- [execute telnet on page 430](#)
- [execute time on page 431](#)
- [execute traceroute on page 431](#)
- [execute tracert6 on page 432](#)
- [execute upload config on page 433](#)
- [execute verify image on page 433](#)
- [execute wake-on-lan on page 434](#)

## execute 802-1x clear mac

Use this command to clear the authorized session associated with the specified MAC address:

```
execute 802-1x clear mac <MAC_address>
```

### Example

This example shows how to remove the authorized session associated with 00:21:cc:d2:76:72:

```
execute 802-1x clear mac 00:21:cc:d2:76:72
```

## execute 802-1x clear interface

Use this command to clear the authorized sessions associated with the specified interface:

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

### Example

This example shows how to remove the authorized sessions associated with port1:

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

## execute 802-1x dacl-clr-stat

Use this command to clear the dynamic access control lists (DACLS) from the specified interface. If the interface is not specified, the DACLS are cleared from all interfaces.

```
execute 802-1x dacl-clr-stat [<interface_name>]
```

### Example

This example shows how to remove DACLS from port 1:

```
execute 802-1x dacl-clr-stat port1
```

## execute 802-1x dacl-reinstall

Use this command to reinstall the DACLS on a specified interface. If the interface is not specified, the DACLS are reinstalled on all interfaces.

```
execute 802-1x dacl-reinstall [<interface_name>]
```

### Example

This example shows how to reinstall the DACLS on port 1:

```
execute 802-1x dacl-reinstall port1
```

## execute acl clear-counter

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

```
execute acl clear-counter {all | ingress | egress | prelookup}
```

Variable	Description
all	Delete the ACL counters for all policies.
ingress	Delete the ACL counters for ingress policies.
egress	Delete the ACL counters for egress policies.
prelookup	Delete the ACL counters for lookup policies.

## Example

This example deletes all ACL counters:

```
execute acl clear-counter all
```

## execute acl key-compaction

**NOTE:** This command currently only works on the ingress policy.

Use the following command to clear the unused classifiers on ASIC hardware associated with ingress, egress, prelookup, or all policies for a particular group:

```
execute acl key-compaction {all | ingress | egress | prelookup} <group_ID>
```

Variable	Description
all	Delete all unused classifiers for the specified group.
ingress	Delete the unused classifiers for ingress policies for the specified group.
egress	Delete the unused classifiers for egress policies for the specified group.
prelookup	Delete the unused classifiers for lookup policies for the specified group.
<group_ID>	Enter the group identifier. Group identifiers are defined in the <code>config switch acl ingress</code> command.

## Example

This example deletes all unused classifiers from group 5:

```
execute acl key-compaction all 5
```

## execute alias configure

Use the `execute alias configure` commands to execute different actions with an alias. The alias is created with the `config system alias command` command with the type set to configuration.

## Syntax

```
execute alias configure get <alias_name> <table-entry-id-if-needed>
```

```
execute alias configure set <alias_name> <table-entry-id-if-needed> <attribute-value>
execute alias configure show <alias_name> <table-entry-id-if-needed>
execute alias configure show-full-configuration <alias_name> <table-entry-id-if-needed>
execute alias configure unset <alias_name> <table-entry-id-if-needed>
```

Variable	Description
get <alias_name> <table-entry-id-if-needed>	Display the current settings.
set <alias_name> <table-entry-id-if-needed> <attribute-value>	Change the attribute to the specified value.
show <alias_name> <table-entry-id-if-needed>	Display an abbreviated version of the current configuration.
show-full-configuration <alias_name> <table-entry-id-if-needed>	Display the full current configuration.
unset <alias_name> <table-entry-id-if-needed>	Reset the attribute to its default value.

## Examples

The following example runs the port-status alias, which displays only the name and status of the specified port (port1 in this example).

```
S548DF5018000776 # execute alias configure get port-status port1
name                : port1
description         : (null)
status              : up
```

The following example changes the value for the port2 table entry to up.

```
S548DF5018000776 # execute alias configure set port-status port2 up
Command to be run:
```

```
-----
config switch physical-port
edit "port2"
set status "up"
next
end
-----
```

Do you want to continue? (y/n)y

The following example displays an abbreviated version of the current configuration for the config switch physical-port command.

```
S548DF5018000776 # execute alias configure show port-status port3
config switch physical-port
  edit "port3"
  next
end
```

The following example displays the full configuration for the config switch physical-port command.

```
S548DF5018000776 # execute alias configure show-full-configuration port-status port4
config switch physical-port
```

```
edit "port4"  
  set description ''  
  set status up  
next  
end
```

The following example toggles the status of port4.

```
548DF5018000776 # execute alias configure unset port-status port4  
Command to be run:
```

```
-----  
config switch physical-port  
  edit "port4"  
    unset status  
  next  
end
```

## execute alias script

Use the `execute alias script` command to run a script that was created with the `config system alias` command with the type set to `script`.

### Syntax

```
execute alias script <script_name> <values...>
```

### Example

This example shows how to run a script named `mac-list` for VLAN 4092.

```
S524DF4K15000024 # execute alias script mac-list 4092  
Command to be run:
```

```
-----  
diag switch mac-address filter clear  
diag switch mac-address filter vlan-map "4092"  
diag switch mac-address list | grep -i mac  
diag switch mac-address filter clear  
-----
```

```
Do you want to continue? (y/n)y
```

```
MAC: 08:5b:0e:f1:95:e5 VLAN: 4092 Port: internal(port-id 31)
```

## execute backup config

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

## Syntax

```
execute backup config flash <comment>
execute backup config ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
    [<password_str>]] [<backup_password_str>]
execute backup config sftp <filename_str> <server_ipv4_ipv6_fqdn> [<username_str> [<password_str>]]
    [<backup_password_str>]
execute backup config tftp <filename_str> <server_ipv4_ipv6_fqdn> [<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_ipv6_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to an FTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the FTP server. Optionally, you can specify a password to protect the saved data.
config sftp <filename_str> <server_ipv4_ipv6_fqdn> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the system configuration to an SFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server. Optionally, you can specify a password to protect the saved data.
config tftp <filename_str> <server_ipv4_ipv6_fqdn> [<backup_password_str>]	Back up the system configuration to a file on a TFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the 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 an FTP, SFTP, or TFTP server.

## Syntax

```
execute backup full-config ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
    [<password_str>]] [<backup_password_str>]
execute backup full-config sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
    [<password_str>]] [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4_ipv6_fqdn> [<backup_password_str>]
```

Variable	Description
full-config ftp <filename_str> <server_ipv4_ipv6_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 use an IPv4 address, IPv6 address, or FQDN to specify the FTP server. You can optionally specify a password to protect the saved data.
full-config sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]	Back up the full system configuration to a file on an SFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server. You can optionally specify a password to protect the saved data.
full-config tftp <filename_str> <server_ipv4_ipv6_fqdn> [<backup_password_str>]	Back up the full system configuration to a file on a TFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the 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 an FTP, SFTP, or TFTP server.

### Syntax

```
execute backup memory alllogs ftp <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]
execute backup memory alllogs sftp <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]
execute backup memory alllogs tftp <server_ipv4_ipv6_fqdn>
execute backup memory log ftp <server_ipv4_ipv6_fqdn[:port_int]> <username_str> <password_str> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}
execute backup memory log sftp <server_ipv4_ipv6_fqdn[:port_int]> <username_str> <password_str> event
execute backup memory log tftp <server_ipv4_ipv6_fqdn> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}
```

Variable	Description
memory alllogs ftp <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]	Back up either all memory or all hard disk log files for to an FTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the FTP server.

Variable	Description
	The disk option is available on FortiSwitch models that log to a hard disk.
memory alllogs sftp <server_ipv4_ipv6_fqdn [:port_int]> [<username_str> <password_str>]	Back up either all memory or all hard disk log files for to an SFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server.  The disk option is available on FortiSwitch models that log to a hard disk.
memory alllogs tftp <server_ipv4_ipv6_fqdn>	Back up either all memory or all hard disk log files for this FortiSwitch to a TFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the TFTP server.  The disk option is available on FortiSwitch models that log to a hard disk.
memory log ftp <server_ipv4_ipv6_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. You can use an IPv4 address, IPv6 address, or FQDN to specify the FTP server.  The disk option is available on FortiSwitch models that log to a hard disk.
memory log sftp <server_ipv4_ipv6_fqdn [:port_int]> <username_str> <password_str> event	Back up the event log file from either hard disk or memory to an SFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server.  The disk option is available on FortiSwitch models that log to a hard disk.
memory log tftp <server_ipv4_ipv6_fqdn> {app-ctrl   event   ids   im   spam   virus   voip   webfilter}	Back up the specified type of log file from either hard disk or memory to a TFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the TFTP 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-snooping

Use these commands to clear the learned and configured IPv4 multicast groups from the FortiSwitch unit. You can combine the commands for more control.

## Syntax

```
execute clear switch igmp-snooping all
execute clear switch igmp-snooping group <multicast_IPv4_address>
execute clear switch igmp-snooping interface <interface_name>
execute clear switch igmp-snooping vlan <VLAN_ID>
```

Variable	Description
all	Clear all IGMP-snooping groups.
group <multicast_IPv4_address>	Clear the specified IGMP-snooping group.
interface <interface_name>	Clear all IGMP-snooping groups on the specified switch interface.
vlan <VLAN_ID>	Clear all IGMP-snooping groups on the specified VLAN.

## Example

The following example clears one IGMP-snooping group from one VLAN for all interfaces:

```
execute clear switch igmp-snooping group 1.2.3.4 100
```

The following example clears one IGMP-snooping group from one VLAN on one interface:

```
execute clear switch igmp-snooping group 1.2.3.4 100 port1
```

The following example clears all IGMP-snooping groups from one interface for one VLAN:

```
execute clear switch igmp-snooping interface port1 100
```

## execute clear switch mld-snooping

Use this command to clear the learned and configured IPv6 multicast groups from the FortiSwitch unit. You can combine the commands for more control.

### Syntax

```
execute clear switch mld-snooping all
execute clear switch mld-snooping group <multicast_IPv6_address>
execute clear switch mld-snooping interface <interface_name>
execute clear switch mld-snooping vlan <VLAN_ID>
```

Variable	Description
all	Clear all MLD-snooping groups.
group <multicast_IPv6_address>	Clear the specified MLD-snooping group.
interface <interface_name>	Clear all MLD-snooping groups on the specified switch interface.
vlan <VLAN_ID>	Clear all MLD-snooping groups on the specified VLAN.

### Example

The following example clears one MLD-snooping group from one VLAN for all interfaces:

```
execute clear switch mld-snooping group ff3f::1 100
```

The following example clears one MLD-snooping group from one VLAN on one interface:

```
execute clear switch mld-snooping group ff3f::1 100 port1
```

The following example clears all MLD-snooping groups from one interface for one VLAN:

```
execute clear switch mld-snooping interface port1 100
```

## execute clear system arp table

Use this command to clear 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 lease-clear

Use these commands to clear DHCP leases:

```
execute dhcp lease-clear all
execute dhcp lease-clear <xxx.xxx.xxx.xxx,yyy.yyy.yyy.yyy,...>
```

Variable	Description	Default
lease-clear all	Clear all DHCP leases.	No default
lease-clear <xxx.xxx.xxx.xxx,yyy.yyy.yyy.yyy,...>	Clear the DHCP leases for the specified IPv4 addresses. Use a comma to separate IPv4 addresses.	No default

## Example

This example shows how to clear all DHCP leases on the specified IPv4 addresses:

```
execute dhcp lease-clear 1.2.3.4,5.6.7.8
```

## execute dhcp lease-list

Use these commands to list DHCP leases:

```
execute dhcp lease-list
execute dhcp lease-list <interface>
```

Variable	Description	Default
lease-list	List all DHCP leases.	No default
lease-list <interface>	List the DHCP leases for the specified interface.	No default

## Example

This example shows how to list all DHCP leases:

```
execute dhcp lease-list
```

## 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 factoryresetfull

Use this command to fully reset the FortiSwitch configuration to factory default settings.

### Syntax

```
execute factoryresetfull
```



This procedure removes all configurations, saved user and application data, and licenses and resets the BIOS environment to the default. Images saved to the partitions are not removed.

---

## execute flapguard reset

Use this command to reset the specified port if flap guard was triggered on that port:

```
execute flapguard reset <port_name>
```

## Example

This example shows how to reset port 1 after flap guard was triggered on it:

```
execute flapguard reset port1
```

## execute fortilink-auth clearstat

Use this command to delete the FortiLink authentication traffic statistics for the port from the FortiSwitch unit:

```
execute fortilink-auth clearstat physical-port <port_name>
```

## execute fortilink-auth reauth

Use this command to reauthenticate FortiLink secured fabric peers from the specified port from the FortiSwitch unit:

```
execute fortilink-auth reauth physical-port <port_name>
```

## execute fortilink-auth reset

Use this command to reset the authentication for the FortiLink secure fabric from the FortiSwitch unit on the specified port:

```
execute fortilink-auth reset physical-port <port_name>
```

## 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 output

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 dhcp6client-renew

Use this command to renew the DHCPv6 client for the specified DHCPv6 interface and close the CLI session. If there is no DHCPv6 connection on the specified port, there is no output.

### Syntax

```
execute interface dhcp6client-renew <interface>
```

## 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.

## Example output

```
S524DF4K15000024 # execute license enhanced-debugging description
This license will enable potentially hazardous debug, such as shells and other features.

S524DF4K15000024 # execute license enhanced-debugging status
enhanced-debugging: Active
Debug license flags: 0x01
```

## execute license status

Use this command to display the status of all installed licenses.

### Syntax

```
execute license status
```

### Example output

```
S524DF4K15000024 # execute license status
License          | Status
enhanced-debugging : Active
FS-SW-LIC-500    : Active
```

## 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 {0 | 1}
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
device {0   1}	Device where the logs are stored. Select 0 for memory or 1 for flash.	0
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 unit, see [config switch global on page 105](#).

## 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 macsec clearstat physical-port

Use this command to clear all MACsec statistics on a single port.

## Syntax

```
execute macsec clearstat physical-port <port_name>
```

## Example

This example shows how to clear the MACsec statistics on port5.

```
#execute macsec clearstat physical-port port5
```

# execute macsec reset physical-port

Use this command to reset the MACsec session on a single port on the server side *or* the client side.

## Syntax

```
execute macsec reset physical-port <port_name>
```

## Example

This example shows how to reset the MACsec session on port5.

```
#execute macsec reset physical-port port5
```

# execute macsec toggle physical-port

Use this command to change the link status and reset the MACsec session on a single port on both the server side *and* the client side. This command applies to the dynamic-CAK mode.

## Syntax

```
execute macsec toggle physical-port <port_name>
```

## Example

This example shows how to change the link status and reset the MACsec session on port5.

```
#execute macsec toggle physical-port port5
```

# execute mtracroute

Use this command to find all the routers that perform load balancing between the FortiSwitch unit and destination.

## Syntax

```
execute mtracroute <IP_address> <confidence_level> <flow_ID> <maximum_hops>
```

Variable	Description
<IP_address>	Enter the IP address to test the connection to.
<confidence_level>	Select the confidence level in percent. You can select 90, 95, or 99. The default value is 95.

Variable	Description
<flow_ID>	<p>Select the flow identifier to use.</p> <p>If you selected an IPv4 address to test, you can select <code>icmp-dst</code>, <code>udp-sport</code>, <code>udp-dst</code>, <code>tcp-sport</code>, or <code>tcp-dst</code> as the flow identifier with <code>udp-sport</code> as the default value.</p> <p>If you selected an IPv6 address to test, you can select <code>icmp-chk</code>, <code>icmp-dst</code>, <code>icmp-fl</code>, <code>icmp-tc</code>, <code>udp-sport</code>, <code>udp-dst</code>, <code>udp-fl</code>, <code>udp-tc</code>, <code>tcp-sport</code>, <code>tcp-dst</code>, <code>tcp-fl</code>, or <code>tcp-tc</code> as the flow identifier with <code>udp-sport</code> as the default value.</p>
<maximum_hops>	Enter the maximum number of hops to test. The range of values is 0-255. The default is 30.

## Example

```
S108FFTV21000010 # execute mtracert 1.2.3.4 90 icmp-chk 50
Run mtracert to 1.2.3.4 - max-ttl: 50, flow-id: icmp-chk, confidence: 90
0 root: 10.105.201.133 (0.767220 ms)
1 10.105.201.133: 192.168.201.1 (0.296219 ms)
2 192.168.201.1: 10.64.254.33 (0.306219 ms)
3 10.64.254.33: 96.45.36.3 (0.501219 ms)
4 96.45.36.3: *
...
```

## 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 adaptive-ping {enable | disable}
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options interface {Auto | <outgoing_interface>}
execute ping-options interval <seconds>
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options reset
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
adaptive-ping {enable   disable}	Enable or disable adaptive ping.	disable
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
interface {Auto   <outgoing_interface>}	Specify the source interface or select auto for the source interface to be automatically assigned.	auto
interval <seconds>	Specify the number of seconds between two pings. The value must be greater than 0.	No default

Variable	Description	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 <code>data_size</code> 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
reset	Reset the ping options to their default settings.	No default
source {auto   <source-intf_ip>}	Specify the FortiSwitch interface from which to send the ping. If you specify <code>auto</code> , the system selects the source address and interface based on the route to the <code>&lt;host-name_str&gt;</code> or <code>&lt;host_ip&gt;</code> . 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: <ul style="list-style-type: none"> <li>• <code>lowdelay</code> – minimize delay</li> <li>• <code>throughput</code> – maximize throughput</li> <li>• <code>reliability</code> – maximize reliability</li> <li>• <code>lowcost</code> – minimize cost</li> </ul>	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
repeat-count <repeats>	Specify how many times to repeat ping.	5

Variable	Description	Default
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: <ul style="list-style-type: none"> <li>• lowdelay – minimize delay</li> <li>• throughput – maximize throughput</li> <li>• reliability – maximize reliability</li> <li>• lowcost – minimize cost</li> </ul>	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 rest list

Use this command to list CMDDB, Monitor, or Execute API endpoints or to find out which endpoints contain a text string.

**NOTE:** You must use the `execute rest login` command before using this command.

### Syntax

```
execute rest list cmdb <[string_to_match]>
execute rest list monitor <[string_to_match]>
execute rest list execute <[string_to_match]>
```

### Example

This example shows how to list all endpoints with the string hardware in them.

```
S524DN4K15000001 # execute rest list monitor hardware
```

No.	Path	Description
[ 1 ]	system/hardware-status	Retrieve Hardware Status of System.
[ 2 ]	hardware/cpu	Retrieve CPU Info of Hardware.

```
[ 3] | hardware/memory | Retrieve Memory Info of Hardware.
```

## execute rest login

Use this command to log in before using the `execute rest` commands. You will be prompted for the administrator user name and the corresponding password.

### Syntax

```
execute rest login
```

### Example

This example shows how to log in to use the `execute rest` commands.

```
S524DN4K15000001 # execute rest login
Enter admin : admin
Enter password : *****
Login success!
```

## execute rest logout

Use this command to log out of the `execute rest` commands.

**NOTE:** You must use the `execute rest login` command before using this command.

### Syntax

```
execute rest logout
```

### Example

This example shows how to log out of the `execute rest` commands.

```
S524DN4K15000001 # execute rest logout
Logged out successfully!
```

## execute rest run

Use this command to run a REST API endpoint.

**NOTE:** You must use the `execute rest login` command before using this command.

### Syntax

```
execute rest run /api/v2/{cmdb | monitor | execute}/<path>/<name> {get | post | put | delete}
<content>
```

### Example

This example shows how to run the GET `/api/v2/monitor/hardware/cpu` endpoint.

```
S524DN4K15000001 # execute rest run /api/v2/monitor/hardware/cpu get
```

```
{
  "http_method": "GET",
  "results": [
    {
      "processor": "0"
    },
    {
      "model name": "ARMv7 Processor rev 0 (v71)"
    },
    {
      "BogoMIPS": "1000.00"
    },
    {
      "Features": "half thumb fastmult edsp tls "
    },
    {
      "CPU implementer": "0x41"
    },
    {
      "CPU architecture": "7"
    },
    {
      "CPU variant": "0x3"
    },
    {
      "CPU part": "0xc09"
    },
    {
      "CPU revision": "0"
    },
    {
      "processor": "1"
    }
  ]
}
```

```
    },
    {
        "model name": "ARMv7 Processor rev 0 (v7l)"
    },
    {
        "BogoMIPS": "1000.00"
    },
    {
        "Features": "half thumb fastmult edsp tls "
    },
    {
        "CPU implementer": "0x41"
    },
    {
        "CPU architecture": "7"
    },
    {
        "CPU variant": "0x3"
    },
    {
        "CPU part": "0xc09"
    },
    {
        "CPU revision": "0"
    },
    {
        "Hardware": "BCM XGS iProc"
    },
    {
        "Revision": "0000"
    },
    {
        "Serial": "0000000000000000"
    }
],
"vdom": "root",
"path": "hardware",
"name": "cpu",
"status": "success",
"cmdb-index": "700",
"cmdb-checksum": "7209412920166404071",
"serial": "S524DN4K1500001",
"version": "v7.2.0",
"build": 393,
"timestamp": "2022-09-13T23:56:12Z"
}
```

## execute rest schema

Use this command to display the schema for the CMDB, Monitor, or Execute API endpoints or for a specific endpoint.

**NOTE:** You must use the `execute rest login` command before using this command.

### Syntax

```
execute rest schema /api/v2/{cmdb | monitor | execute}[/<path>/<name>]
```

### Example

This example shows how to display the schema for the `/api/v2/monitor/hardware/cpu` endpoint.

```
execute rest schema /api/v2/monitor/hardware/cpu
```

```
{
  "schema": [
    {
      "url": "/api/v7.2.0/monitor/hardware/cpu",
      "path": "hardware",
      "name": "cpu",
      "schema": {
        "name": "cpu",
        "category": "table",
        "help": "Retrieve CPU Info of Hardware.",
        "children": {
          "name": {
            "name": "name",
            "category": "unitary",
            "type": "string",
            "help": "Hardware's CPU Attribute Name."
          },
          "value": {
            "name": "value",
            "category": "unitary",
            "type": "string",
            "help": "Hardware's CPU Attribute Value."
          }
        }
      }
    }
  ],
  "cmdb-index": "700",
  "cmdb-checksum": "7209412920166404071",
  "serial": "S524DN4K15000001",
  "version": "v7.2.0",
  "build": 393,
  "timestamp": "2022-09-13T23:08:51Z",
```

```
"action": "schema",
"status": "success"
}
```

## execute restore bios

Use this command to restore the BIOS from a file on a TFTP server. You can use an IPv4 address, IPv6 address, or FQDN to specify the TFTP server.

### Syntax

```
execute restore bios tftp <filename_str> <server_ipv4_ipv6_fqdn>
```

### Example

This example shows how to restore the BIOS from a file on a TFTP server. The name of the BIOS file on the TFTP server is bios. The IP address of the TFTP server is 192.168.1.23.

```
execute restore bios tftp bios 192.168.1.23
```

## execute restore config

Use this command to restore the configuration from a file on the flash disk or on an FTP, SFTP, or TFTP server.

### Syntax

```
execute restore config flash <revision>
execute restore config ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
    <password_str>] [<backup_password_str>]
execute restore config sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
    <password_str>] [<backup_password_str>]
execute restore config tftp <filename_str> <server_ipv4_ipv6_fqdn> [<backup_password_str>]
```

Variable	Description
config flash <revision>	Restore the specified revision of the system configuration from the flash disk.
config ftp <filename_str> <server_ipv4_ipv6_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.

Variable	Description
	<p>You can use an IPv4 address, IPv6 address, or FQDN to specify the FTP server.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config sftp &lt;filename_str&gt; &lt;server_ipv4_ ipv6_fqdn[:port_int]&gt; [&lt;username_str&gt; &lt;password_str&gt;] [&lt;backup_password_str&gt;]</pre>	<p>Restore the system configuration from an SFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server.</p> <p>If the backup file was created with a password, you must specify the password.</p>
<pre>config tftp &lt;filename_str&gt; &lt;server_ipv4_ ipv6_fqdn&gt; [&lt;backup_password_str&gt;]</pre>	<p>Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords.</p> <p>You can use an IPv4 address, IPv6 address, or FQDN to specify the TFTP server.</p> <p>If the backup file was created with a password, you must specify the password.</p>

## Example

The following example shows how to download a configuration file from a TFTP server to the FortiSwitch unit 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
```

The following example shows how to download a configuration file from an SFTP server to the FortiSwitch unit and restart the FortiSwitch unit with this configuration. The name of the configuration file on the SFTP server is backupconfig. The IPv6 address of the SFTP server is 6001:7:7:7::2, and the port number is 2222. To access the SFTP server, you need to add the user name, admin, and the password, adminpassword.

```
execute restore config sftp backupconfig 6001:7:7:7::2]:2222 admin adminpassword
```

## execute restore image

Use this command to change the FortiSwitch firmware.

### Syntax

```
execute restore image ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
<password_str>]
execute restore image management-station <version_int>
```

```
execute restore image sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
<password_str>]
execute restore image tftp <filename_str> <server_ipv4_ipv6_fqdn> [<source_ipv4_ipv6>]
```

Variable	Description
image ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]	Download a firmware image from an FTP server to the FortiSwitch unit. The FortiSwitch unit reboots, loading the new firmware. You can use an IPv4 address, IPv6 address, or FQDN to specify the FTP server.
image management-station <version_int>	Download a firmware image from the central management station. This command is available only 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 sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]	Download a firmware image from an SFTP server to the FortiSwitch unit. The FortiSwitch unit reboots, loading the new firmware. You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server.
image tftp <filename_str> <server_ipv4_ipv6_fqdn> [<source_ipv4_ipv6>]	Download a firmware image from a TFTP server to the FortiSwitch unit. The FortiSwitch unit reboots, loading the new firmware. You can use an IPv4 address, IPv6 address, or FQDN to specify the TFTP server. You can use an IPv4 or IPv6 address to specify an optional source IP address.

## Example

The following example shows how to download an image file from a TFTP server to the FortiSwitch unit. The name of the image file on the TFTP server is `build0914`. The IP address of the TFTP server is `192.168.1.23`.

```
execute restore image tftp build0914 192.168.1.23
```

The following example shows how to download an image file from an SFTP server to the FortiSwitch unit. The name of the image file on the SFTP server is `build0813`. The IPv6 address of the SFTP server is `6001:7:7:7::2`, and the port number is `2222`. To access the SFTP server, you need to add the user name, `admin`, and the password, `adminpassword`.

```
execute restore image sftp build0813 6001:7:7:7::2:2222 admin adminpassword
```

## execute restore license

Use this command to download a new license file from an FTP, SFTP, or TFTP server.

## Syntax

```
execute restore license ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
<password_str>]
execute restore license sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str>
<password_str>]
execute restore license tftp <filename_str> <server_ipv4_ipv6_fqdn>
```

Variable	Description
license ftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]	Download a license file from an FTP server to the FortiSwitch unit. You can use an IPv4 address, IPv6 address, or FQDN to specify the FTP server.
license sftp <filename_str> <server_ipv4_ipv6_fqdn[:port_int]> [<username_str> <password_str>]	Download a license file from an SFTP server to the FortiSwitch unit. You can use an IPv4 address, IPv6 address, or FQDN to specify the SFTP server.
license tftp <filename_str> <server_ipv4_ipv6_fqdn>	Download a license file from a TFTP server to the FortiSwitch unit. You can use an IPv4 address, IPv6 address, or FQDN to specify the TFTP server.

## Examples

The following example shows how to download a license file from a TFTP server to the FortiSwitch unit. The name of the license file on the TFTP server is `newlicense`. The IP address of the TFTP server is `192.168.1.23`.

```
execute restore license tftp newlicense 192.168.1.23
```

The following example shows how to download a license file from an SFTP server to the FortiSwitch unit. The name of the license file on the SFTP server is `newlicense`. The IPv6 address of the SFTP server is `6001:7:7:7::2`, and the port number is `2222`. To access the SFTP server, you need to add the user name, `admin`, and the password, `adminpassword`.

```
execute restore license sftp newlicense 6001:7:7:7::2]:2222 admin adminpassword
```

## 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 clear bgp

Use these commands to clear the BGP routing configuration.

### Syntax

```
execute router clear bgp all <arguments>
execute router clear bgp as <arguments>
execute router clear bgp dampening <IP_address>
execute router clear bgp dampening <IP_address/length>
execute router clear bgp external <arguments>
execute router clear bgp ip <A.B.C.D|X::X::X:X|*>
execute router clear bgp ipv6 <A.B.C.D|X::X::X:X|*>
```

Variable	Description
all <arguments>	Clear all BGP peers
as <arguments>	Clear a BGP peer by AS number.
dampening <IP_address>	Clear the BGP flap-dampening information.
dampening <IP_address/length>	Clear the BGP flap-dampening information.
external <arguments>	Clear all external BGP peers.
ip <A.B.C.D X::X::X:X *>	Clear a BGP peer by IPv4 or IPv6 address. Use * to clear all BGP peers.
ipv6 <A.B.C.D X::X::X:X *>	Clear a BGP peer by IPv4 or IPv6 address. Use * to clear all BGP peers.

## Example

Use the following command to delete the BGP flap-dampening information:

```
execute router clear bgp dampening 1.2.3.4
```

## execute router clear evpn dup-addr

Use these commands to clear the EVPN duplicate MAC addresses.

### Syntax

```
execute router clear evpn dup-addr vni all
execute router clear evpn dup-addr vni <VNI_number>
execute router clear evpn dup-addr vni <VNI_number> mac <MAC_address>
```

Variable	Description
vni all	Clear all duplicate MAC addresses.
vni <VNI_number>	Clear the duplicate MAC addresses in the specified VXLAN network identifier (VNI).
vni <VNI_number> mac <MAC_address>	Clear the specified MAC address in the specified VNI.

## execute router clear ospf

Use this command to clear the OSPF routing configuration from the specified interface.

### Syntax

```
execute router clear ospf interface <interface_name>
```

### Example

Use the following command to delete the OSPF routing configuration from the VLAN interface:

```
execute router clear ospf interface vlan20
```

## execute router tech-support

Use this command to display the specified routing configuration and troubleshooting information.

### Syntax

```
execute router tech-support {ospf | rip | bgp | isis | static}
```

## Example

Use the following command to display the BGP routing configuration and troubleshooting information:

```
execute router tech-support bgp
```

## execute set-next-reboot

Use this command to specify the flash partition for the next reboot. The system can use the boot image from either the primary or the secondary flash partition.

**NOTE:** You must disable image rotation before you can use the `execute set-next-reboot` command.

## Syntax

```
execute set-next-reboot <primary | secondary>
```

## Example

This example specifies that the next reboot will use the secondary flash partition:

```
execute set-next-reboot secondary
Set next reboot partition to 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 source-guard-violation reset

Use these commands to reset the source-guard violations.

### Syntax

```
execute source-guard-violation reset all
execute source-guard-violation reset interface <interface_name>
```

Variable	Description
all	Reset all source-guard violations.
interface <interface_name>	Reset source-guard violations for the specified switch interface.

## 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@IPv4\_address, user@IPv6\_address, or user@DNS\_name. If the IPv6 address is a link-local address, you must specify an output interface using %.

### Examples

```
execute ssh admin@fe80::926c:acff:fe7b:e059%vlan20 // vlan20 is the output interface.
execute ssh admin@172.20.120.122
```

```
execute ssh 1002::21
execute ssh 12.345.6.78
```

To end an SSH session, type exit:

```
S524DF4K15000024 # exit
Connection to 172.20.120.122 closed.
S524DF4K15000024 #
```

## execute ssh-regen-keys

Use this command to regenerate SSH server keys.



After you enter the command, the SSH server restarts, and the current SSH connections are disconnected.

### Syntax

```
execute ssh-regen-keys
```

### Example

```
S448ENTF21000633 # execute ssh-regen-keys
SSH server will restart and current SSH connections will be disconnected!
Do you want to continue? (y/n)y
Keys regenerated, sshd restarting...
```

## execute stage

Use this command to download a firmware image from an FTP, SFTP, or TFTP server and stage it without restarting the FortiSwitch unit.

### Syntax

```
execute stage image ftp <string> <ftp server>[:ftp port] [<FTP_user_name> <FTP password>]
execute stage image sftp <string> <sftp server>[:sftp port] <SFTP_user_name> <SFTP password>
execute stage image tftp <string> <tftp server> [<source_IPv4_IPv6_address>]
```

<string> is the image file name (including path) on the remote server.

You can use an IPv4 address, IPv6 address, or fully qualified domain name to identify the server.

## Example

This example shows how to stage an image from an SFTP server.

```
execute stage image sftp build0914 192.168.1.23 admin mypassword
```

## 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 clear-nac-mac-cache

Use this command to delete the FortiSwitch cache of network access control (NAC) MAC addresses.

### Syntax

```
execute switch-controller clear-nac-mac-cache
```

## execute switch-controller delete-nac-mac-cache

Use this command to delete a specify MAC address in the FortiSwitch NAC cache.

## Syntax

```
execute switch-controller delete-nac-mac-cache <MAC_address>
```

## Example

```
S524DF4K15000024 # execute switch-controller delete-nac-mac-cache 00:00:02:00:0d:00
```

# 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 unit is managed by a FortiGate device.

## Syntax

```
execute switch-controller get-conn-status
```

## Example

```
S524DF4K15000024 # execute switch-controller get-conn-status
```

```
Get managed-switch S524DF4K15000024 connection status:  
Connection: Connected  
Image Version: FG100D-v6.2-build849  
Remote Address: xxx.xxx.x.x  
Join Time: Wed Mar 13 08:38:57 2019  
DTLS Version: DTLSv1.2
```

# execute switch-controller get-nac-mac-cache

Use this command to list the MAC addresses in the FortiSwitch NAC cache.

## Syntax

```
execute switch-controller get-nac-mac-cache
```

## Example

```
S548DN5018000532 # execute switch-controller get-nac-mac-cache

MAC-ADDRESS VLAN ACT SYNC INTERFACE

00:00:02:00:0d:00 4089 1 0 port2
00:00:02:00:0d:01 4089 1 0 port2
00:00:02:00:0d:02 4089 1 0 port2
```

## execute system admin account-convert-sha1

Use this command to convert the password for a system administrator account to SHA1 encryption.

### Syntax

```
execute system admin account-convert-sha1 <admin_name>
```

### Example

```
S524DF4K15000024 # execute system admin account-convert-sha1 localadmin
```

## execute system admin account-convert-sha256

Use this command to convert the password for a system administrator account to SHA256 encryption.

### Syntax

```
execute system admin account-convert-sha256 <admin_name>
```

### Example

```
S524DF4K15000024 # execute system admin account-convert-sha256 localadmin
```

## 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
import	Import the CA certificate from a TFTP server to the FortiSwitch unit.
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
import	Import the CRL from the configured LDAP, HTTP, or SCEP authentication server to the FortiSwitch unit.
<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 unit 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 ec

Use this command to request an elliptic curve (ECDSA) certificate.

### Syntax

```
execute system certificate local generate ec <name> <elliptical_curve_name> <subject_str> <country>
<state> <city> <organization> <bu> <email> <SAN> <URL> <challenge> <source_IP> <CA_id>
<password>
```

Variable	Description
<name>	Enter the local certificate name.
<elliptical_curve_name>	Enter the elliptical curve name, which can be secp256r1, secp384r1, or secp521r1.

Variable	Description
<subject_str>	Enter the subject (host IP address/domain name/e-mail address).
<country>	Enter the country name (such as canada), country code (such as ca), or null for none.
<state>	Enter the state.
<city>	Enter the city.
<organization>	Enter the company name.
<bu>	Enter the business unit.
<email>	Enter the email address.
<SAN>	This field is optional. Enter a subject alternative name.
<URL>	This field is optional. Enter the URL of the CA server for signing using SCEP.
<challenge>	Enter the challenge password for signing using SCEP.
<source_IP>	This field is optional. Enter the source IP address for communicating with the CA server.
<CA_id>	This field is optional. Enter the CA identifier of the CA server for sign using SCEP.
<password>	This field is optional. Enter the password if you are using a private key.

## execute system certificate local generate rsa

Use this command to request a Rivest-Shamir-Adleman (RSA) certificate.

When you request an RSA certificate, you create a private and public key pair for the local FortiSwitch unit. 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 unit.

### Syntax

```
execute system certificate local generate rsa <name> <key-length> <subject_str> <country> <state>
<city> <organization> <bu> <email> <SAN> <URL> <challenge> <source_IP> <CA_id> <password>
```

Variable	Description
<name>	Enter the local certificate name.
<key-length>	Enter the key size, which can be 1024, 1536, 2048, or 4096.
<subject_str>	Enter the subject (host IP address/domain name/e-mail address).

Variable	Description
<country>	Enter the country name (such as canada), country code (such as ca), or null for none.
<state>	Enter the state.
<city>	Enter the city.
<organization>	Enter the company name.
<bu>	Enter the business unit.
<email>	Enter the email address.
<SAN>	This field is optional. Enter a subject alternative name.
<URL>	This field is optional. Enter the URL of the CA server for signing using SCEP.
<challenge>	Enter the challenge password for signing using SCEP.
<source_IP>	This field is optional. Enter the source IP address for communicating with the CA server.
<CA_id>	This field is optional. Enter the CA identifier of the CA server for sign using SCEP.
<password>	This field is optional. Enter the password if you are using a private key.

## 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
<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 unit to a TFTP server. The remote certificates are public certificates without a private key. They are used as

OCS (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
import	Import the remote certificate from the TFTP server to the FortiSwitch unit.
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 remote certificate.
<file-name>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.

## execute system sniffer-profile delete-capture

Use this command to delete the .pcap file for a specific packet-capture profile. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

### Syntax

```
execute system sniffer-profile delete-capture <profile_name>
```

### Example

```
execute system sniffer-profile delete-capture profile1
```

## execute system sniffer-profile pause

Use this command to pause a packet capture for a specific packet-capture profile. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

## Syntax

```
execute system sniffer-profile pause <profile_name>
```

## Example

```
execute system sniffer-profile pause profile1
```

# execute system sniffer-profile start

Use this command to start a packet capture for a specific packet-capture profile. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

## Syntax

```
execute system sniffer-profile start <profile-name>
```

## Example

```
execute system sniffer-profile start profile1
```

# execute system sniffer-profile stop

Use this command to stop a packet capture for a specific packet-capture profile. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

## Syntax

```
execute system sniffer-profile stop <profile-name>
```

## Examples

```
execute system sniffer-profile stop profile1
```

## execute system sniffer-profile upload

Use this command to upload the .pcap file for a specific packet-capture profile to a TFTP or FTP server. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

### Syntax

```
execute system sniffer-profile upload ftp <profile_name> <file_name> <FTP_server_IP_
address:<optional_port>>
execute system sniffer-profile upload tftp <profile_name> <file_name> <TFTP_server_IP_
address:<optional_port>>
```

Variable	Description
<profile_name>	Enter the name of the packet-capture profile.
<file_name>	Enter the name of the .pcap file and the path where it is located.
<FTP_server_IP_address:<optional_port>>	Enter the IP address of the FTP server and optionally enter the port number.
<TFTP_server_IP_address:<optional_port>>	Enter the IP address of the TFTP server and optionally enter the port number.

### Examples

```
execute system sniffer-profile upload ftp profile profile1.pcap 192.168.1.23
```

## execute telnet

Use this command to create a Telnet client. You can use this tool to test network connectivity.

### Syntax

```
execute telnet <telnet_ipv4 or telnet_ipv6>
```

<telnet\_ipv4 or telnet\_ipv6> is the IPv4 or IPv6 address to connect with. If the IPv6 address is a link-local address, you must specify an output interface using %.

Type exit to close the Telnet session.

### Examples

```
execute telnet fe80::926c:acff:fe7b:e059%vlan20 // vlan20 is the output interface.
execute telnet 1002::21
```

```
execute telnet 12.345.6.78
```

## 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 {<IPv4_address> | <host-name>} <maximum_number_of_hops> <number_of_probes>
<maximum_number_of_milliseconds>
```

Variable	Description	Default
{<IPv4_address>   <host-name>}	Enter the IPv4 address or host name to trace the route to.	

Variable	Description	Default
<maximum_number_of_hops>	Enter the maximum number of hops that the route can take.	32
<number_of_probes>	Enter the number of probes to use to trace the route.	3
<maximum_number_of_milliseconds>	Enter how many milliseconds a route can take before the trace route is stopped.	5 seconds

## Example

This example shows how to test the connection with <http://docs.forticare.com>. In this example, the traceroute command times out after the fifth hop indicating a possible problem.

```
S548DF5018000776 # execute traceroute docs.forticare.com 10 5 10
traceroute to docs.forticare.com (208.91.114.175), 10 hops max, 5 probe count, 10 timeout, 72 byte
packets
 1  10.105.16.1  0.765 ms  0.415 ms  0.170 ms  0.164 ms  6.952 ms
 2  10.64.254.33 1.687 ms  0.666 ms  2.438 ms  2.048 ms  0.289 ms
 3  96.45.36.3   1.767 ms  0.630 ms  0.281 ms  0.323 ms  0.257 ms
 4  96.45.47.219 21.311 ms 21.403 ms 23.585 ms 21.232 ms 21.414 ms
 5  96.45.47.14  20.783 ms 20.730 ms 21.269 ms 20.747 ms 20.730 ms
 6  * * * * *
```

If your FortiSwitch is not connected to a working DNS server, you will not be able to connect to remote host-named locations with the traceroute command.

## 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.

Variable	Description
-i <interface>	Select interface to use for tracer.
-m <max_ttl>	Set the max time-to-live (max number of hops) used in outgoing probe packets.
-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
```

# execute wake-on-lan

Use this command to send Wake-on-LAN (WoL) packets to a specific MAC address to remotely turn on a computer.

## Syntax

```
execute wake-on-lan <interface_type> <interface_or_port> <host_MAC_address> <protocol> <port> <IP_<br>address> <password>
```

Variable	Description
<interface_type>	Select the interface type that will send the WoL packets. Select 1 if to use the system interface or 2 to use the switch port. The default is 1.
<interface_or_port>	If you selected 1 for the interface type, specify which system interface to use (required). If you selected 2 for the interface type, specify which switch port to use (optional).
<host_MAC_address>	Required. Enter the MAC address (XX:XX:XX:XX:XX:XX) of the computer that needs to be turned on.
<protocol>	Optional. Select which protocol to use to send the WoL packets. Select 1 for WoL or 2 for UDP. The default is 2.
<port>	Optional. If you selected 2 for the protocol, select which port the WoL packets will use. You can select 0, 7, or 9. The default is 9.
<IP_address>	Optional. If you selected 2 for the protocol, enter the broadcast IP address used by the WoL packets.

Variable	Description
<password>	Optional. Enter the password if a 6-byte SecureOn password is enabled on the destination host. The password can be a string or 0x plus a hexadecimal value.

## Examples

If you are sending the WoL packets by UDP from the FortiSwitch port3 to a MAC address of aa:bb:cc:00:11:22:

```
execute wake-on-lan 2 port3 aa:bb:cc:00:11:22 2 9 1.2.3.4
```

If you are sending the WoL packets by UDP from the FortiSwitch port10 to a MAC address of 10:20:30:40:50:60 and the destination host is protected by a SecureOn password:

```
execute wake-on-lan 2 port10 10:20:30:40:50:60 2 9 10.10.10.10 passwd
```

# get

The `get` commands provide information about the operation of the FortiSwitch unit:

- [get hardware cpu on page 438](#)
- [get hardware memory on page 439](#)
- [get hardware status on page 440](#)
- [get log custom-field on page 440](#)
- [get log eventfilter on page 441](#)
- [get log gui on page 442](#)
- [get log memory on page 442](#)
- [get log syslogd on page 443](#)
- [get log syslogd2 on page 444](#)
- [get log syslogd3 on page 445](#)
- [get router info bfd neighbor on page 446](#)
- [get router info bgp on page 446](#)
- [get router info evpn on page 447](#)
- [get router info gwdetect on page 448](#)
- [get router info isis on page 448](#)
- [get router info kernel on page 449](#)
- [get router info pbr on page 449](#)
- [get router info multicast on page 450](#)
- [get router info ospf on page 451](#)
- [get router info rip on page 453](#)
- [get router info routing-table on page 454](#)
- [get router info vrrp on page 455](#)
- [get router info6 bfd neighbor on page 456](#)
- [get router info6 bgp on page 456](#)
- [get router info6 isis on page 457](#)
- [get router info6 kernel on page 457](#)
- [get router info6 ospf on page 458](#)
- [get router info6 rip on page 459](#)
- [get router info6 routing-table on page 459](#)
- [get router info6 vrrp on page 460](#)
- [get switch acl on page 461](#)
- [get switch dhcp-snooping on page 462](#)
- [get switch flapguard settings on page 464](#)
- [get switch global on page 464](#)
- [get switch igmp-snooping on page 465](#)
- [get switch interface on page 466](#)
- [get switch ip-mac-binding on page 467](#)
- [get switch ip-source-guard on page 467](#)
- [get switch ip-source-guard-violations on page 468](#)

- [get switch lldp on page 468](#)
- [get switch mac-limit-violations on page 469](#)
- [get switch mirror status on page 470](#)
- [get switch mld-snooping on page 471](#)
- [get switch modules on page 472](#)
- [get switch mrp on page 474](#)
- [get switch network-monitor on page 473](#)
- [get switch phy-mode on page 475](#)
- [get switch physical-port on page 475](#)
- [get switch poe inline on page 476](#)
- [get switch qos on page 477](#)
- [get switch rguard-policy on page 477](#)
- [get switch security-feature on page 478](#)
- [get switch static-mac on page 478](#)
- [get switch storm-control on page 479](#)
- [get switch stp instance on page 479](#)
- [get switch stp settings on page 480](#)
- [get switch trunk on page 480](#)
- [get switch virtual-wire on page 481](#)
- [get switch vlan on page 481](#)
- [get system accprofile on page 482](#)
- [get system admin list on page 482](#)
- [get system admin status on page 483](#)
- [get system arp on page 484](#)
- [get system arp-table on page 484](#)
- [get system bug-report on page 484](#)
- [get system certificate on page 485](#)
- [get system cmdb status on page 486](#)
- [get system console on page 487](#)
- [get system dns on page 487](#)
- [get system flan-cloud on page 488](#)
- [get system flan-cloud-mgr connection-info on page 488](#)
- [get system flow-export on page 490](#)
- [get system flow-export-data on page 491](#)
- [get system global on page 491](#)
- [get system info admin ssh on page 492](#)
- [get system info admin status on page 493](#)
- [get system interface physical on page 493](#)
- [get system interface vlan on page 494](#)
- [get system interface vxlan on page 495](#)
- [get system ipv6-neighbor-cache on page 496](#)
- [get system link-monitor on page 496](#)
- [get system location on page 496](#)
- [get system ntp on page 497](#)
- [get system password-policy on page 497](#)

- [get system performance firewall statistics on page 498](#)
- [get system performance status on page 498](#)
- [get system performance top on page 499](#)
- [get system schedule group on page 500](#)
- [get system schedule onetime on page 500](#)
- [get system schedule recurring on page 501](#)
- [get system settings on page 501](#)
- [get system sflow on page 502](#)
- [get system sniffer-profile capture on page 502](#)
- [get system sniffer-profile summary on page 502](#)
- [get system snmp sysinfo on page 503](#)
- [get system source-ip status on page 503](#)
- [get system startup-error-log on page 504](#)
- [get system status on page 504](#)
- [get test on page 505](#)
- [get user group on page 506](#)
- [get user ldap on page 506](#)
- [get user local on page 506](#)
- [get user radius on page 507](#)
- [get user setting on page 507](#)
- [get user tacacs+ on page 508](#)

## get hardware cpu

Use this command to display detailed information about the CPUs installed in your FortiSwitch unit.

### 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

```
S524DF4K1500024 # 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 21](#).

## 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 24](#).

## 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	<p>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.</p> <ul style="list-style-type: none"> <li>emergency – The system is unusable.</li> <li>alert – Immediate action is required.</li> <li>critical – Functionality is affected.</li> <li>error – An erroneous condition exists and functionality is probably affected.</li> <li>warning – Functionality might be affected.</li> <li>notification – Information about normal events.</li> <li>information – General information about system operations.</li> <li>debug – Information used for diagnosing or debugging the system.</li> </ul>
global-setting	<p>Find out the global settings for logging to system memory:</p> <ul style="list-style-type: none"> <li>full-final-warning-threshold – the number of log entries saved before a final</li> </ul>

Variable	Description
	<p>warning is sent. When all memory is filled, the system overwrites the oldest log entries.</p> <ul style="list-style-type: none"> <li>• <code>full-first-warning-threshold</code> – the number of log entries saved before receiving the first warning.</li> <li>• <code>full-second-warning-threshold</code> – the number of log entries saved for receiving the second warning.</li> <li>• <code>hourly-upload</code> – whether the log is uploaded hourly.</li> <li>• <code>max-size</code> – the maximum size of the memory buffer log, in bytes.</li> </ul>
setting	<p>Find out the general settings for logging to system memory:</p> <ul style="list-style-type: none"> <li>• <code>diskfull</code> – whether the oldest log entries are overwritten when the system memory is full.</li> <li>• <code>status</code> – whether logging to system memory is enabled.</li> </ul>

## 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 <code>error</code> , the system logs <code>error</code> , <code>critical</code> , <code>alert</code> , and <code>emergency</code> .

Variable	Description
	<p>level messages.</p> <ul style="list-style-type: none"> <li>• <b>emergency</b> – The system is unusable.</li> <li>• <b>alert</b> – Immediate action is required.</li> <li>• <b>critical</b> – Functionality is affected.</li> <li>• <b>error</b> – An erroneous condition exists and functionality is probably affected.</li> <li>• <b>warning</b>– Functionality might be affected.</li> <li>• <b>notification</b> – Information about normal events.</li> <li>• <b>information</b> – General information about system operations.</li> <li>• <b>debug</b> – Information used for diagnosing or debugging the system.</li> </ul>
setting	<p>Find out the general settings for the system log 1:</p> <ul style="list-style-type: none"> <li>• <b>diskfull</b> – whether the oldest log entries are overwritten when the system memory is full.</li> <li>• <b>status</b> – whether logging to system memory is enabled.</li> </ul>

## 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	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>emergency</b> – The system is unusable.</li> <li>• <b>alert</b> – Immediate action is required.</li> <li>• <b>critical</b> – Functionality is affected.</li> <li>• <b>error</b> – An erroneous condition exists and functionality is probably affected.</li> <li>• <b>warning</b>– Functionality might be affected.</li> </ul>

Variable	Description
	<ul style="list-style-type: none"> <li>notification – Information about normal events.</li> <li>information – General information about system operations.</li> <li>debug – Information used for diagnosing or debugging the system.</li> </ul>
setting	Find out the general settings for the system log 2: <ul style="list-style-type: none"> <li>diskfull – whether the oldest log entries are overwritten when the system memory is full.</li> <li>status – whether logging to system memory is enabled.</li> </ul>

## 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. <ul style="list-style-type: none"> <li>emergency – The system is unusable.</li> <li>alert – Immediate action is required.</li> <li>critical – Functionality is affected.</li> <li>error – An erroneous condition exists and functionality is probably affected.</li> <li>warning – Functionality might be affected.</li> <li>notification – Information about normal events.</li> <li>information – General information about system operations.</li> <li>debug – Information used for diagnosing or debugging the system.</li> </ul>
setting	Find out the general settings for the system log 3: <ul style="list-style-type: none"> <li>diskfull – whether the oldest log entries are overwritten when the</li> </ul>

Variable	Description
	system memory is full. <ul style="list-style-type: none"> <li>status – whether logging to system memory is enabled.</li> </ul>

## Example output

```
S524DF4K15000024 # get log syslogd3 filter
severity          : information

S524DF4K15000024 # get log syslogd3 setting
status           : disable
```

## get router info bfd neighbor

Use this command to find out where bidirectional forwarding detection (BFD) has been enabled. If you do not specify the BFD peer IPv4 address or interface, all BFD peers are returned.

### Syntax

```
get router info bfd neighbor [<BFD_local_IPv4_address>] [<BFD_peer_interface>]
```

### 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 bgp

Use this command to get information about the Border Gateway Protocol (BGP) routing configuration.

### Syntax

```
get router info bgp {cidr-only | community | community-info | community-list | dampening | filter-
list | neighbors | network | network-longer-prefixes | paths | prefix-list | regexp | route-
map | summary | evpn}
```

Variable	Description
cidr-only	Display routes with nonnatural netmasks.
community	Display routes matching the communities.
community-info	List all BGP community information.
community-list	Display routes matching the community list.
dampening	Display router dampening information.
filter-list	Display routes conforming to the filter list.
neighbors	Show BGP neighbors for IPv4 and IPv6.
network	Show the BGP information for the network.
network-longer-prefixes	Show the BGP information for routes and more specific routes.
paths	Display the BGP path information for IPv4 and IPv6.
prefix-list	Display routes conforming to the prefix list.
regexp	Display routes matching the AS path with regular expressions.
route-map	Display routes conforming to the route map.
summary	Display a summary of the BGP neighbor status for IPv4 and IPv6.
evpn	Display the Ethernet Virtual Private Network (EVPN) information.

## get router info evpn

Use these commands to get information about the Ethernet Virtual Private Network (EVPN) .

### Syntax

```
get router info evpn vni detail
get router info evpn vni <VNI_number>
get router info evpn arp-cache vni [<VNI_number>]
get router info evpn mac vni dup-addr
get router info evpn mac vni <VNI_number>
get router info evpn arp-nd-proxy-stats vni <VNI_number>
```

Variable	Description
vni detail	Show information about all VXLAN network identifiers (VNIs).
vni <VNI_number>	Show information about the specified VXLAN network identifier (VNI).
arp-cache vni [<VNI_number>]	Show the ARP and ND cache for the specified

Variable	Description
	VNI. If the VNI is not specified, results for all configured VNIs are shown.
mac vni dup-addr	Show all duplicate MAC addresses.
mac vni <VNI_number>	Show the MAC addresses for the specified VNI.
arp-nd-proxy-stats vni <VNI_number>	Show the ARP and ND proxy statistics for the specified VNI.

## get router info gwdetect

Use this command to get information about the gwdetect status.

### Syntax

```
get router info gwdetect
```

## get router info isis

Use this command to get information about the Intermediate System to Intermediate System Protocol (IS-IS) routing configuration for IPv4 traffic.

### Syntax

```
get router info isis {interface | neighbor | database | route | summary | summary-table | topology}
```

Variable	Description
interface	Show the IS-IS interfaces.
neighbor	Show the IS-IS neighbor adjacencies.
database	Show the IS-IS link state database.
route	Show the IS-IS IP routing table.
summary	Show the IS-IS summary.
summary-table	Show the IS-IS IPv4 summary table.
topology	Show the IS-IS paths.

## get router info kernel

Use this command to get information about the IPv4 kernel routing table. The IPv4 kernel routing table displays information about all of the routes in the kernel.

### Syntax

```
get router info kernel <routing_type>
```

## get router info pbr

Use these commands to get information about the policy-based routing (PBR) configuration.

### Syntax

```
get router info pbr {map | nexthop-group}
```

Variable	Description
map ["<map-name> <sequence-number> <interface-name>"]	Show the specified PBR rule. If the PBR rule is not specified , all rules are returned.
nexthop-group	Show the PBR next-hop group.

### Example output

```
S524DF4K15000024 # get router info pbr map
pbr-map pbrmap1
  Seq: 1 rule: 300 Installed: 0 UniqIdx: 1 HardwareInstalled: 0 Reason: Invalid NH-group
    SRC Match: 22.1.1.0/24
    DST Match: 0.0.0.0/0
    Nexthop-Group: 12:1:1:2:(10001) Installed: 0(0)
  Seq: 2 rule: 301 Installed: 0 UniqIdx: 2 HardwareInstalled: 0 Reason: Invalid NH-group
    SRC Match: 0.0.0.0/0
    DST Match: 33.1.1.0/24
    Nexthop-Group: nhgroup1(10000) Installed: 0(0)
  Seq: 3 rule: 302 Installed: 0 UniqIdx: 4 HardwareInstalled: 0 Reason: Invalid NH-group
    SRC Match: 11.1.1.0/24
    DST Match: 0.0.0.0/0
    Nexthop-Group: 13:1:1:2:vrfv4(10002) Installed: 0(0)

S524DF4K15000024 # get router info pbr nexthop-group
```

```

NextHop-Group: 12:1:1:2: Table: 10001 Valid: 0 Installed: 0
Valid: 0 nexthop 12.1.1.2
NextHop-Group: nhgroup1 Table: 10000 Valid: 0 Installed: 0
Valid: 0 nexthop 12.1.1.4
Valid: 0 nexthop 12.1.1.5
NextHop-Group: 13:1:1:2:vrfv4 Table: 10002 Valid: 0 Installed: 0
Valid: 0 nexthop 13.1.1.2 nexthop-vrf vrfv4

```

## get router info multicast

Use this command to get information about the Protocol Independent Multicast (PIM) routing configuration.

### Syntax

```
get router info multicast {config | igmp | pim | table | table-count | info}
```

Variable	Description
config	Show the multicast routing configuration.
igmp { groups   sources   interface <interface_name>   join }	Show the multicast routing IGMP information.
pim { neighbour   interface <interface_name>   assert   assert-internal   assert-metric   assert-winner-metric   join   local-membership   rpf   secondary   upstream   upstream-join-desired   upstream-rpf }	Show PIM information.
table	Show the multicast routing table.
table-count	Show the multicast route and packet count.
info	Show the IP multicast.

### Example output

```

S524DF4K15000024 # get router info multicast info
Router MLAG Role: NONE
Mroute socket descriptor: 7(default)
Mroute socket uptime: 180164:50

Zclient update socket: 11 failures=0
Zclient lookup socket: 12 failures=0

Maximum highest VifIndex: 255

Upstream Join Timer: 60 secs

```

```
Join/Prune Holdtime: 210 secs
PIM ECMP: Disable
PIM ECMP Rebalance: Disable
```

```
RPF Cache Refresh Delay: 50 msecs
RPF Cache Refresh Timer: 0 msecs
RPF Cache Refresh Requests: 0
RPF Cache Refresh Events: 0
RPF Cache Refresh Last: --:--:--
NextHop Lookups: 0
NextHop Lookups Avoided: 0
```

```
Scan OIL - Last: --:--:-- Events: 0
MFC Add - Last: --:--:-- Events: 0
MFC Del - Last: --:--:-- Events: 0
```

Interface	Address	ifi	Vif	PktsIn	PktsOut	BytesIn	BytesOut
-----------	---------	-----	-----	--------	---------	---------	----------

## get router info ospf

Use this command to get information about any IPv4 open shortest path first (OSPF) routing that has been configured. To set up IPv4 OSPF routing, see [config router ospf on page 60](#).

### Syntax

```
get router info ospf config
get router info ospf redist-route
get router info ospf summary
get router info ospf database {brief | self-originate | router | network | summary | asbr-summary |
    external | nssa-external | opaque-link | opaque-area | opaque-as | max-age}
get router info ospf interface [<interface_name>]
get router info ospf route
get router info ospf neighbor {<neighbor_ID> | all | detail | detail all | <interface_IP_address>}
get router info ospf border-routers
get router info ospf status
get router info ospf vrf <VRF_name>
```

Variable	Description
config	Display detailed information about the current OSPF configuration, including interfaces, areas, access lists, and IP addresses.
redist-route	Display information about the OSPF redistributed routes.
summary	Display summary table information.

Variable	Description
database {brief   self-originate   router   network   summary   asbr-summary   external   nssa-external   opaque-link   opaque-area   opaque-as   max-age}	Display information about the OSPF database.
interface [<interface_name>]	Display information about the specified OSPF interface. If the interface is not specified, information about all OSPF interfaces is returned.
route	Display the OSPF routing table.
neighbor {<neighbor_ID>   all   detail   detail all   <interface_IP_address>}	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.
vrf <VRF_name> {rdist-route   summary   database   interface   route   neighbor   border-routers   status}	Display virtual routing and forwarding (VRF) information within OSPF.

## Example output

```
S524DF4K1500024 # 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 millise(c)s
Minimum hold time between consecutive SPF(s) 10000 millise(c)s
Maximum hold time between consecutive SPF(s) 10000 millise(c)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 76](#).

### Syntax

```
get router info rip {config | database | status}
```

Variable	Description
config	Display detailed information about the current RIP configuration, including keys in the key chain, 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 these commands to get information about the IPv4 routing table.

### Syntax

```

get router info routing-table <IPv4_address_route_prefix>
get router info routing-table summary
get router info routing-table all
get router info routing-table rip
get router info routing-table ospf
get router info routing-table bgp
get router info routing-table isis
get router info routing-table static
get router info routing-table connected
get router info routing-table vrf <VRF_name>
get router info routing-table dump <A.B.C.D>

```

Variable	Description
<IPv4_address_route_prefix>	Display the routes for the specified IP address or route prefix.
summary	Display a summary of the existing routes.
all	Display all routing table entries.
rip	Display the RIP routes in the routing table.
ospf	Display the OSPF routes in the routing table.
bgp	Display the BGP routes in the routing table.
isis	Display the IS-IS routes in the routing table.
static	Display the static routes in the routing table.

Variable	Description
connected	Display the connected routes in the routing table.
vrf <VRF_name>	Display the VRF routes in the routing table.
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 summary
Route Source      Routes      FIB (vrf default)
connected         3           3
static            1           1
-----
Totals            4           4

S524DF4K15000024 # get router info routing-table all
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route ^ - HW install failed

S>* 0.0.0.0/0 [5/0] via 169.254.1.1, internal, 00:36:02
C>* 10.254.252.0/23 is directly connected, rspan, 00:34:37
C>* 169.254.1.0/24 is directly connected, internal, 1d00h57m
C>* 192.168.2.0/24 is directly connected, mgmt, 01:51:05
```

## get router info vrrp

Use this command to get information about Virtual Router Redundancy Protocol (VRRP) groups for IPv4.

### 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 info6 bfd neighbor

Use this command to find out where bidirectional forwarding detection (BFD). If you do not specify the BFD peer IPv6 address, all BFD peers are returned.

### Syntax

```
get router info6 bfd neighbor [<X:X::X:X>]
```

## get router info6 bgp

Use this command to get information about the Border Gateway Protocol (BGP) routing configuration.

### Syntax

```
get router info6 bgp {community | community-list | dampening | filter-list | neighbors | network |
network-longer-prefixes | paths | prefix-list | regexp | route-map | summary}
```

Variable	Description
community	Display routes matching the communities.
community-list	Display routes matching the community list.
dampening	Display router dampening information.
filter-list	Display routes conforming to the filter list.
neighbors	Show BGP neighbors.
network	Show the BGP information for the network.
network-longer-prefixes	Show the BGP information for routes and more specific routes.
paths	Display the BGP path information.
prefix-list	Display routes conforming to the prefix list.
regexp	Display routes matching the AS path with regular expressions.
route-map	Display routes conforming to the route map.

Variable	Description
summary	Display a summary of the BGP neighbor status.

## get router info6 isis

Use this command to get information about the Intermediate System to Intermediate System Protocol (IS-IS) routing configuration for IPv6 traffic.

### Syntax

```
get router info6 isis {interface | neighbor | database | route | summary | summary-table6 | topology}
```

Variable	Description
interface	Show the IS-IS interfaces.
neighbor	Show the IS-IS neighbor adjacencies.
database	Show the IS-IS link state database.
route	Show the IS-IS IP routing table.
summary	Show the IS-IS summary.
summary-table 6	Show the IS-IS IPv6 summary table.
topology	Show the IS-IS paths.

## get router info6 kernel

Use this command to get information about the IPv6 kernel routing table. The IPv6 kernel routing table displays information about all of the routes in the kernel.

### Syntax

```
get router info6 kernel
```

### Example output

```
S524DF4K1500024 # get router info6 kernel
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::/128 gwy::: prio=0
```

```

type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::/128 gwy:: prio=0
type=02 protocol=unspec flag=00000000 oif=1(lo) dst:fe80::/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=01 protocol=kernel flag=00000000 oif=42(internal) dst:fe80::/64 prio=100
type=01 protocol=kernel flag=00000000 oif=2(mgmt) dst:fe80::/64 prio=100
type=01 protocol=kernel flag=00000000 oif=49(rspan) dst:fe80::/64 prio=100
type=01 protocol=boot flag=00000000 oif=42(internal) dst:ff00::/8 prio=100
type=01 protocol=boot flag=00000000 oif=2(mgmt) dst:ff00::/8 prio=100
type=01 protocol=boot flag=00000000 oif=49(rspan) dst:ff00::/8 prio=100
type=07 protocol=kernel flag=00000000 oif=1(lo) prio=ffffffff

```

## get router info6 ospf

Use this command to get information about any IPv6 open shortest path first (OSPF) routing that has been configured. To set up IPv6 OSPF routing, see [config router ospf6 on page 68](#).

### Syntax

```

get router info6 ospf database [{router | network | inter-prefix | inter-router | external | link |
    intra-prefix}]
get router info6 ospf interface [<interface_name>]
get router info6 ospf route [<IPv6_address>]
get router info6 ospf redistribute
get router info6 ospf border-route [detail]
get router info6 ospf neighbor {<A.B.C.D> | detail}
get router info6 ospf status

```

Variable	Description
database [{router   network   inter-prefix   inter-router   external   link   intra-prefix}]	Display information about the OSPF link state advertisement (LSA) database. Specify the router LSA, network LSA, inter-prefix LSA, inter-router LSA, external LSA, link LSA, or intra-prefix LSA database. If you do not specify which LSA database, information about all LSA databases is returned.
interface [<interface_name>]	Display information about the OSPF interface. If you do not specify the interface, information about all interfaces is returned.
route [<IPv6_address>]	Display the OSPF routing table. If you do not specify an IPv6 address, all IPv6 routes are returned.
redistribute	Display redistributing external information.
border-route [detail]	Display general or detailed information about OSPF border routers.
neighbor {<A.B.C.D>   detail}	Display information about OSPF neighbors in general or in detail or specify a neighbor ID.

Variable	Description
status	Display the current status of the OSPF routing, including router identifier, flags, timers, and areas.

## get router info6 rip

Use this command to get information about any IPv6 Routing Information Protocol (RIP) routing that has been configured. To set up IPv6 RIP routing, see [config router ripng on page 80](#).

### Syntax

```
get router info6 rip config
get router info6 rip database
get router info6 rip status
```

Variable	Description
config	Display information about the RIP configuration.
database	Display information about the RIP routes.
status	Display the current status of the RIP routing, including timers, filter lists, and neighbors.

## get router info6 routing-table

Use these commands to get information about the IPv6 routing table. If you do not specify which IPv6 routing table, information about all IPv6 routing tables is returned.

### Syntax

```
get router info6 routing-table <IPv6_address_route_prefix>
get router info6 routing-table rip
get router info6 routing-table isis
get router info6 routing-table ospf
get router info6 routing-table bgp
get router info6 routing-table static
get router info6 routing-table connected
get router info6 routing-table vrf <VRF_name>
```

Variable	Description
<IPv6_address_route_prefix>	Display the routes for the specified IPv6 address or prefix.
rip	Display the RIP routes in the routing table.
isis	Display the ISIS routes in the routing table.
ospf	Display the OSPF routes in the routing table.
bgp	Display the BGP routes in the routing table.
static	Display the static routes in the routing table.
connected	Display the connected routes in the routing table.
vrf <VRF_name>	Display the VRF routes in the routing table.

## Example output

```
S524DF4K15000024 # get router info6 routing-table
Codes: K - kernel route, C - connected, S - static, R - RIPng,
O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
f - OpenFabric,
> - selected route, * - FIB route, q - queued route, r - rejected route ^ - HW install failed

C * fe80::/64 is directly connected, rspan, 02:41:19
C * fe80::/64 is directly connected, mgmt, 03:56:28
C>* fe80::/64 is directly connected, internal, 1d03h03m
K>* ff00::/8 [0/256] is directly connected, rspan, 02:41:20
```

## get router info6 vrrp

Use this command to get information about Virtual Router Redundancy Protocol (VRRP) groups for IPv6.

### Syntax

```
get router info6 vrrp
```

### Example output

```
S548DF4K15000007 # get router info6 vrrp
vrrp_ctx_dump_status: icl_tr: icl_trid:-1
Interface: port26, primary IPv6 address: 2000::30:44:0:5
link-local IPv6 address: fe80::a5b:eff:fee5:5321
```

```

Virtual link-local IPv6 address: fe80::30:44:0:1
  UseVMAC: 1
  VRID: 10 version: 3
    vrip: 2000::30:44:0:1, priority: 100, state: BACKUP
    adv_interval: 1, preempt: 1, start_time: 3
    master_adv_interval: 100, accept: 1
    vrmac: 00:00:5e:00:02:0a
    vrdst:
    vrgrp: 0

Interface: vlan30, primary IPv6 address: 2000::30:0:0:5
link-local IPv6 address: fe80::a5b:eff:fee5:5307
Virtual link-local IPv6 address: fe80::30:0:0:1
  UseVMAC: 1
  VRID: 10 version: 3
    vrip: 2000::30:0:0:1, priority: 100, state: MASTER
    adv_interval: 1, preempt: 1, start_time: 3
    master_adv_interval: 100, accept: 1
    vrmac: 00:00:5e:00:02:0a
    vrdst:
    vrgrp: 0

```

## get switch acl

Use these commands to display the ACL settings.

### Syntax

```

get switch acl counters {all | egress | ingress | prelookup}
get switch acl egress
get switch acl ingress
  get switch acl policer
get switch acl prelookup
  get switch acl service custom
  get switch acl settings
get switch acl usage

```

Variable	Description
counters {all   egress   ingress   prelookup}	Display information about all ACL policies, egress ACL policies, ingress ACL policies, or lookup ACL policies.
egress	Display information about the ACL policy for the egress stage.
ingress	Display information about the ACL policy for the ingress stage.
policer	List which ACL policers are available for different types of traffic.
prelookup	Display information about the ACL policy for the lookup stage.

Variable	Description
service custom	Display a list of preconfigured service entries .
settings	Display the global ACL settings for the FortiSwitch unit.
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      STAGE
(total/free) (total/free) (total/free)
-----
0       2048 /2023  4096 /4071  4096 /4096  ingress
0       512  /511   1024 /1024  768  /768   egress
0       768  /767   0    /0     0    /0     prelookup

S524DF4K15000024 # get switch acl counters ingress
ingress:
ID      Packets      Bytes      description
-----
0001 0            0          cnt_n_mirror13
0002 0            0          cnt_n_mirror31
0003 0            0          cnt_n_mirror41
```

## get switch dhcp-snooping

Use these commands to display more information about the IPv4 or IPv6 DHCP-snooping databases.

### Syntax

```
get switch dhcp-snooping allowed-sever-list
get switch dhcp-snooping client-db-details
get switch dhcp-snooping client6-db-details
get switch dhcp-snooping database-summary
get switch dhcp-snooping limit-db-details
get switch dhcp-snooping server-db-details
```

```
get switch dhcp-snooping server6-db-details
get switch dhcp-snooping static-clients
get switch dhcp-snooping status
```

Variable	Description
allowed-sever-list	Display the allowed DHCP server list.
client-db-details	Display the details about the IPv4 DHCP-snooping client database.
client6-db-details	Display the details about the IPv6 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 the details about the DHCP-snooping lease-count database.
server-db-details	Display the details about the IPv4 DHCP-snooping server database. If the dhcp-server-access-list is enabled globally and the server is configured for the dhcp-server-access-list, the svr-list column displays allowed for that server. If the dhcp-server-access-list is enabled globally and the server is not configured in the dhcp-server-access-list, the svr-list column displays blocked for that server.
server6-db-details	Display the details about the IPv6 DHCP-snooping server database. If the dhcp-server-access-list is enabled globally and the server is configured for the dhcp-server-access-list, the svr-list column displays allowed for that server. If the dhcp-server-access-list is enabled globally and the server is not configured in the dhcp-server-access-list, the svr-list column displays blocked for that server.
static-clients	Display the details about the DHCP-snooping static client database.
status	Display details about the DHCP-snooping client and server database.

## Example output

```
S548DF5018000776 # get switch dhcp-snooping allowed-server-list
```

```

vlan      ip
10        xxx.x.x.x
```

```
FS1D243Z14000027 # get switch dhcp-snooping client-db-details
```

```

mac      vlan  ip      lease(sec) expiry
(sec) interface hostname domainname vendor server-ip
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 svr-list last-seen-time expiry-
time OFFER/ACK/NAK/OTHER
00:11:01:00:00:01 10 xxx.x.x.x port1 trusted allowed 2018-09-11 11:21:09 2018-09-
12 11:21:09 7/5/0/0

```

```
get switch dhcp-snooping static-clients
```

S	MAC Address	VLAN	Client IP	Lease Time(D:H:M:S)	Expiry Time(D:H:M:S)
	Interface	Host Name	Domain Name	Vendor	Server IP
*	00:01:00:00:00:01	10	10.1.1.1*	Infinity	Infinity
	port3	1			0.0.0.0

## get switch flapguard settings

Use this command to display the flap guard settings.

### Syntax

```
get switch flapguard settings
```

### Example output

```

S524DF4K1500024 # 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 unit.

### 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-is1            : enable
mclag-peer-info-timeout: 300
auto-is1-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 unit.

### Syntax

```
get switch igmp-snooping {globals | group | static-group | status}
```

Variable	Description
globals	Display the global IGMP-snooping configuration on the FortiSwitch unit.
group	Display a list of learned multicast groups.
static-group	Display the list of configured static groups.
status	Display the status of IGMP-snooping VLANs and group

## Example output

```
S524DF4K15000024 # get switch igmp-snooping globals
aging-time : 300
leave-response-timeout: 10
query-interval : 120
```

```
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-snooping 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

```
S524DF4K15000048 # get switch igmp-snooping status
```

```
IGMP-SNOOPING enabled vlans:
-----
100
```

```
IGMP-Proxy enabled vlans:
-----
```

```
Max multicast snooping groups 1022
```

```
Total IGMP groups 0 (Learned 0, Static 0)
Total MLD groups 0 (Learned 0, Static 0)
```

```
Remaining allowed mcast snooping groups: 1022
```

## 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 ip-source-guard

Use this command to get information about the IP source-guard entries.

## Syntax

```
get switch ip-source-guard
```

# get switch ip-source-guard-violations

Use these commands to get source-guard violations.

## Syntax

```
get switch ip-source-guard-violations all
get switch ip-source-guard-violations interface <interface_name>
```

Variable	Description
all	Display all source-guard violations.
interface <interface_name>	Display source-guard violations for the specified interface.

# 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 <port_name>	Display statistics and status 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.

Variable	Description
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 network-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 unit, see [config switch global on page 105](#).

### 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 status

Use this command to get information about the ERSPAN-auto mirror sessions of your FortiSwitch unit. To configure a packet mirror, see [config switch mirror on page 138](#).

### Syntax

```
get switch mirror status <session>
```

### Example output

```
# get switch mirror status flink.sniffer
```

```
flink.sniffer
Mode : ERSPAN-auto
Status : Inactive
Source-Ports:
  Ingress: port2, port3
  Egress : port8, port9
Used-by-ACLs : False
Auto-config-state : N/A
Last-update : never
Issues : None
Collector-IP : 0.0.0.0
Source-IP : N/A
Source-MAC : N/A
Next-Hop :
  IP : N/A
  MAC : N/A
  Via-System-Interface : N/A
```

VLAN : N/A  
Via-Switch-Interface : N/A

## get switch mld-snooping

Use this command to get the MLD-snooping settings of your FortiSwitch unit.

### Syntax

```
get switch mld-snooping {globals | group | static-group | status}
```

Variable	Description
globals	Display the global MLD-snooping configuration on the FortiSwitch unit.
group	Display a list of learned multicast groups.
static-group	Display the list of configured static groups.
status	Display the status of MLD-snooping VLANs and group

### Example output

```
S548DF5018000776 # get switch mld-snooping globals
```

```
aging-time : 300
leave-response-timeout: 10
query-interval : 125
```

```
S548DF5018000776 # get switch mld-snooping group
```

```
MLD-SNOOPING mcast-groups:
Max Entries: 1022
```

```
port VLAN GROUP Age-timeout MLD-Version
```

```
Total Number of Learned MLD groups: 0
```

```
S548DF5018000776 # get switch mld-snooping static-group
```

```
VLAN ID Group-Name Multicast-addr Member-interface
```

---

```
S548DF5018000776 # get switch mld-snooping status
```

```
MLD-SNOOPING enabled vlans:
-----
40
```

```
MLD-Proxy enabled vlans:
-----
```

40

Max multicast snooping groups 1022

Total MLD groups 0 (Learned 0, Static 0)

Total IGMP groups 0 (Learned 0, Static 0)

Remaining allowed mcast snooping groups: 1022

## get switch modules

Use this command to get information about the modules in your FortiSwitch unit.

### Syntax

```
get switch modules {detail | limits | status | summary} [<port>]
```

Variable	Description
detail [<port>]	Display module details for a specific port, split port, or all available ports.
limits [<port>]	Display module limits for a specific port, split port, or all available ports.
status [<port>]	Display module status for a specific port, split port, or all available ports.
summary [<port>]	Display summary information of all modules for a specific port or all available ports and split ports.

### Example output

```
S148FNTF20000098 # get switch modules detail port50
```

```

Port(port50)
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
vendor_sn      PU71L2H
manuf_date     08/15/2015

```

```
FS1E48T419000004 # get switch modules status port50
```

```

Port(port50)
temperature    23.957031 C
voltage        3.293100 volts
alarm_flags[0] 0x0000
warning_flags[0] 0x0000
laser_bias[0]  0.761600 mAmps
tx_power[0]    -2.246809 dBm
rx_power[0]    -2.926854 dBm
alarm_flags[1] 0x0000
warning_flags[1] 0x0000
laser_bias[1]  0.755200 mAmps
tx_power[1]    -1.993517 dBm
rx_power[1]    -3.300326 dBm
alarm_flags[2] 0x0000
warning_flags[2] 0x0000
laser_bias[2]  0.761600 mAmps
tx_power[2]    -2.105603 dBm
rx_power[2]    -2.486439 dBm
alarm_flags[3] 0x0000
warning_flags[3] 0x0000
laser_bias[3]  0.748800 mAmps
tx_power[3]    -2.128939 dBm
rx_power[3]    -2.641617 dBm
options        0x000F ( TX_DISABLE TX_FAULT RX_LOSS TX_POWER_LEVEL1 )
options_status 0x0008 ( TX_POWER_LEVEL1 )

```

## get switch network-monitor

Use this command to get information about network monitoring on the FortiSwitch unit.

### 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 mrp

Use these commands to get information about the Media Redundancy Protocol (MRP) configuration.

### Syntax

```
get switch mrp {profile | settings}
```

Variable	Description
profile	List the available MRP profiles.
settings	Display the MRP settings.

## Example output

```
SR24DN4416000049 # get switch mrp profile
== [ 500ms ]
name: 500ms
== [ MRPprofile1 ]
name: MRPprofile1

SR24DN4416000049 # get switch mrp settings
status          : disable
role            : client
domain-id       : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF
domain-name     : domain1
vlan-id         : 1
priority        : 40960
ring-port1      : (null)
ring-port2      : (null)
profile-name    : 500ms
```

## 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 146.

### 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 unit. To configure physical ports, see [config switch physical-port](#) on page 148.

### 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 raguard-policy

Use the following command to list the available IPv6 RA-guard policies. To create an IPv6 RA-guard policy, see [config switch raguard-policy on page 161](#).

### Syntax

```
get switch raguard-policy
```

## Example output

```
S524DF4K15000024 # get switch raguard-policy
== [ RApolicy1 ]
name: RApolicy1
```

# 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 163.

## 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

```
S524DF4K1500024 # 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 unit. To configure storm control, see [config switch storm-control on page 167](#).

### Syntax

```
get switch storm-control
```

## Example output

```
S524DF4K1500024 # 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 unit. To configure an STP instance, see [config switch stp instance on page 167](#).

### 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 unit. To configure STP settings, see [config switch stp settings on page 169](#).

### 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 unit have been configured for link aggregation. To configure link aggregation, see [config switch trunk on page 170](#).

### 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 174](#).

### 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 unit. To configure a VLAN, see [config switch vlan on page 174](#).

### 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 185](#).

### 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 187](#).

### 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 unit. To manually add ARP table entries to the FortiSwitch unit, see [config system arp-table on page 195](#).

### 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 unit.

### 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 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 201](#).

## 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 ocsf
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 unit.

### Syntax

```
get system cmdb status
```

Variable	Description
version	Version of the CMDB software.
owner id	Process identifier of the CMDB server daemon.
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 206](#).

### 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 213](#).

### 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 flan-cloud

Use this command to display the configuration for FortiLAN Cloud or FortiLink with HTTPS management.

### Syntax

```
get system flan-cloud
```

### Example output

```
S524DF4K15000024 # get system flan-cloud

interval        : 3
name            : fortiswitch-dispatch.forticloud.com
service-type    : flan-cloud
port            : 443
status          : enable
```

## get system flan-cloud-mgr connection-info

Use this command to check your connection to FortiLAN Cloud or FortiLink with HTTPS.

### Syntax

```
get system flan-cloud-mgr connection-info
```

## Example output

```
S224DF3X15000367 # get system flan-cloud-mgr connection-info

Service Name: : FortiLink
User Account-ID : 0
SSL verify Code : ok
Access Service : IP= 30.30.30.25, Port= 443, Connected on: 2023-10-17 14:07:44
Bootstrap Service : hostname= , Port= 0

State-Machine : State= FLAN_MGR_STATE_READY, Event= EV_READY_SSL_SESSION_ESTD

SSL Local End-Point : Interface: internal, IP: 20.20.20.4
SSL Tunnel Uptime : Days: 2 Hours: 6 Mins: 22 [Connected @2023-10-17 14:07:44]
SSL Tunnel stats : restart-count= 31, Restart Reason= Admin Shutdown

Stats:
=====
Switch Keep Alive Tx/Reply := 5808 / 5808
Manager Keep Alive Rx/Error := 14795 / 0

Socks Req Rx/Last Stream-ID := 127621 / 5
Reset Req Rx/last Stream-ID := 6717 / 13462
Goaway Req Rx := 0
Unknown Req Rx := 0

Syslog FD/Tx/Err := 10 / 1 / 0

Fortilink details
=====
stream_id : 5
online state_id : 9
localSock fd : 11
stpTelSock fd : 12
dhcpTelSock fd : 13
igmpsTelSock fd : 14
macSock fd : 15
cmfSock fd : 16
TX counter : 8
RX_ACK counter : 8
RX_NACK counter : 0
topology req : 11616
topology resp : 11616
system telemetry req : 10096
system telemetry resp : 10096
interface telemetry req : 4
interface telemetry resp : 4
mac telemetry req : 5620
mac telemetry resp : 5620
dot1x user req : 0
dot1x user resp : 0
lldp nbr req : 0
```

```
lldp nbr resp : 0
mac cache req : 0
mac cache resp : 0
trunk state req : 34843
trunk state resp : 34843
port state req : 5810
port state resp : 5810
poe status req : 5807
poe status resp : 5807
```

Used SOCKS stream-id:

=====

SID SockFd Proxy-Ports State Description

---

```
1 0 UNKNOWN:0<-->0 DATA BOOTSTRAP
3 0 UDP:9514<-->0 DATA SYSLOG DATA
5 0 UNKNOWN:0<-->0 DATA FORTILINK
```

## get system flow-export

Use this command to display the flow-export configuration. To configure flow export, see [config system flow-export](#) on page 215.

### Syntax

```
get system flow-export
```

### Example output

```
S524DF4K15000024 # get system flow-export
aggregates:
collector-ip       : 0.0.0.0
collector-port    : 0
format            : ipfix
identity          : 0x00000000
level             : ip
max-export-pkt-size : 512
timeout-general   : 3600
timeout-icmp      : 300
timeout-max       : 604800
timeout-tcp       : 3600
timeout-tcp-fin   : 300
timeout-tcp-rst   : 120
```

```
timeout-udp      : 300
transport       : tcp
```

## get system flow-export-data

Use this command to display the flow-export data. To configure flow export, see [config system flow-export](#) on page 215.

### Syntax

```
get system flow-export-data flows {all | <count>} {ip | subnet | mac | all} <switch_interface_name>
get system flow-export-data flows-raw {all | <count>} {ip | subnet | mac | all} <switch_interface_name>
get system flow-export-data statistics
```

**NOTE:** Layer-2 flows for netflow 1 and netflow 5 are not supported. For the output of the `get system flow-export-data statistics` command, the Incompatible Type field displays how many flows are not exported because they are not supported.

Variable	Description
flows {all   <count>} {ip   subnet   mac   all} <switch_interface_name>	Display the specified number of records or all records of flow data for the specified IP address, subnet (class IP address and netmask), MAC address, or all.
flows-raw {all   <count>} {ip   subnet   mac   all} <switch_interface_name>	Display the specified number of records or all records of raw flow data for the specified IP address, subnet (class IP address and netmask), MAC address, or all.
statistics	Display the statistics for the flow data.

## get system global

Use this command to get the global settings of your FortiSwitch unit. To configure global settings, see [config system global](#) on page 218.

### 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
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 unit 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 unit.

## 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

```
S524DF4K1500024 # 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 interface vlan

Use this command to list information about the VLAN interfaces.

## Syntax

```
get system interface vlan
```

## Example output

```
S224ENTF18000826 # get system interface vlan

== [vlan]
  ==[15]
    mode: static
    ip: 1.2.3.4 255.255.255.0
    ipv6: ::/0
    status: up
```

```
rx : 0 bytes  0 packets
tx : 36576 bytes  863 packets
==[vlan10]
mode: static
ip: 2.3.4.5 255.255.255.0
ipv6: ::/0
status: up
rx : 0 bytes  0 packets
tx : 792 bytes  11 packets
==[vlan11]
mode: static
ip: 3.4.5.6 255.255.255.0
ipv6: ::/0
status: up
rx : 0 bytes  0 packets
tx : 792 bytes  11 packets
==[vlan12]
mode: static
ip: 4.5.6.7 255.255.255.0
ipv6: ::/0
status: up
rx : 0 bytes  0 packets
tx : 792 bytes  11 packets
==[vlan13]
mode: static
ip: 5.6.7.8 255.255.255.0
ipv6: ::/0
status: up
rx : 0 bytes  0 packets
tx : 792 bytes  11 packets
```

## get system interface vxlan

Use this command to list information about the VXLAN interfaces.

### Syntax

```
get system interface vxlan
```

### Example output

```
S524DF4K16000028 # get system interface vxlan

== [vxlan]
    ==[vni.200]
        mode: static
```

```
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: down
rx : 0 bytes 0 packets
tx : 0 bytes 0 packets
```

## get system ipv6-neighbor-cache

Use this command to list information about the IPv6 neighbor cache table. To configure the IPv6 neighbor cache table, see [config system ipv6-neighbor-cache on page 238](#).

### Syntax

```
get system ipv6-neighbor-cache
```

## 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 239](#).

### Syntax

```
get system link-monitor
```

## get system location

Use this command to get information about the location table used by LLDP-MED for enhanced 911 emergency calls. To configure a location table, see [config system location on page 240](#).

### Syntax

```
get system location
```

### Example output

```
S548DF5018000776 # get system location
== [ Fortinet ]
name: Fortinet
```

## get system ntp

Use this command to get information about the NTP settings. To configure an NTP server, see [config system ntp](#) on page 244.

### 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 245.

### 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.

### Example output

```
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
initXXXXXXXXXX  1       S      0.0    0.5
newcli          1040    S <    0.0    0.5
ipconflict      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 schedule group

Use this command to list available schedule groups for when an access control list (ACL) will be active. To configure a schedule group, see [config system schedule group on page 250](#).

### Syntax

```
get system schedule group
```

### Example output

```
S548DF501800776 # get system schedule group
== [ group1 ]
name: group1
```

## get system schedule onetime

Use this command to list available one-time schedules for when an access control list (ACL) will be active. To configure a one-time schedule, see [config system schedule onetime on page 251](#).

## Syntax

```
get system schedule onetime
```

## Example output

```
S548DF5018000776 # get system schedule onetime
== [ schedule1 ]
name: schedule1
```

# get system schedule recurring

Use this command to list schedules for when an access control list (ACL) will be active every week. To configure a recurring schedule, see [config system schedule recurring on page 251](#).

## Syntax

```
get system schedule recurring
```

## Example output

```
S548DF5018000776 # get system schedule recurring
== [ schedule2 ]
name: schedule2
```

# 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 252](#).

## 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 253](#).

### Syntax

```
get system sflow
```

### Example output

```
S524DF4K15000024 # get system sflow
```

```
collector-ip      : 0.0.0.0  
collector-port    : 6343
```

## get system sniffer-profile capture

Use this command to display the packet capture for a specific packet-capture profile. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

### Syntax

```
get system sniffer-profile capture <profile_name>
```

## get system sniffer-profile summary

Use this command to display the status of all configured packet-capture profiles. To create a packet-capture profile, see [config system sniffer-profile on page 254](#).

### Syntax

```
get system sniffer-profile summary
```

### Example output

```
S524DF4K15000024 # get system sniffer-profile summary
```

```
Maximum memory available for storing packet-capture: 100 MB.
```

```
Name | Status | Pkt-Count | Snap Len | Size (KB) | Filter
=====
profile1 | Stop | No Capture | 100 | 0.00 | none
```

## 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 257.

### Syntax

```
get system snmp sysinfo
```

### Example output

```
S524DF4K1500024 # 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 IP addresses.

### 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 the following:

- firmware version, build number, and branch point
- serial number
- whether the firmware signature is verified
- BIOS version
- host name
- system part number
- system time and date

### Syntax

```
get system status
```

### Example output

```
S224ENTF18000826 # get system status
```

```
Version: FortiSwitch-224E v7.4.0,build0752,230410 (Interim)
Serial-Number: S224ENTF18000826
Firmware Signature: invalid
Boot: Coldboot
```

```

BIOS version: 04000015
System Part-Number: P21932-03
Burn in MAC: 70:4c:a5:c8:7f:82
Hostname: S224ENTF18000826
Distribution: International
Branch point: 752
System time: Wed Apr 12 16:34:42 2023

```

## get test

Use this command to display information about applications on this FortiSwitch unit:

### Syntax

```
get test {dnsproxy | fpmdd | radiusd | sflowd | snmpd} <test_level_int>
```

Variable	Description
{dnsproxy   fpmdd   radiusd   sflowd   snmpd}	Set the application to be tested. Tests can be run on the following applications: <ul style="list-style-type: none"> <li>• dnsproxy – DNS proxy</li> <li>• fpmdd – FPM daemon</li> <li>• radiusd – RADIUS daemon</li> <li>• sflowd – sFlow daemon</li> <li>• snmpd – SNMP daemon</li> </ul>
<test_level_int>	Set the level for the test.

### Example output

```

S524DF4K15000024 # get test fpmdd 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 264](#).

### 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 266](#).

### 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 268](#).

### 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 270](#).

### 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
```

# sleep

Use this command to add a delay in a script.

## Syntax

```
sleep <1-172800 seconds>
```

## Example

```
sleep 10
```

# Appendix: FortiSwitch QoS template

The following is a template for setting up QoS on a FortiSwitch unit:

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

config switch qos ip-dscp-map
  edit "voice-dscp"
    config map
      edit "1"
        set cos-queue 1
        set value 46
      next
      edit "2"
        set cos-queue 2
        set value 24,26,48,56
      next
      edit "5"
        set cos-queue 3
        set value 34
      next
    end
  next
end

config switch qos qos-policy
  edit "default" // you can ignore this portion, this is default policy
    config cos-queue
      edit "queue-0"
      next
      edit "queue-1"
      next
      edit "queue-2"
      next
      edit "queue-3"
      next
      edit "queue-4"
      next
    end
end
```

```
                edit "queue-5"
                next
                edit "queue-6"
                next
                edit "queue-7"
                next
            end
        set schedule round-robin
    next
    edit "voice_egr_policy"
        config cos-queue
            edit "queue-0"
            next
            edit "queue-1"
                set weight 0
            next
            edit "queue-2"
                set weight 6
            next
            edit "queue-3"
                set weight 37
            next
            edit "queue-4"
                set weight 12
            next
            edit "queue-5"
            next
            edit "queue-6"
            next
            edit "queue-7"
            next
        end
    set schedule weighted
next
end

edit "port5"
    ...
    set trust-dot1p-map " voice-dot1p "
    set trust-ip-dscp-map " voice-dscp "
next
edit "port6"
    ...
    set trust-dot1p-map " voice-dot1p "
    set trust-ip-dscp-map " voice-dscp "
next
edit "port7"
    ...
    set trust-dot1p-map " voice-dot1p "
    set trust-ip-dscp-map " voice-dscp "
next
end
```

```
edit "port14"  
  ...  
  set qos-policy "voice_egr_policy"  
end
```



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.