

FortiSwitchOS Administration Guide— Standalone Mode

Version 6.2.5

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET KNOWLEDGE BASE

<http://kb.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET NSE INSTITUTE (TRAINING)

<https://training.fortinet.com/>

FORTIGUARD CENTER

<https://fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT AND PRIVACY POLICY

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

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

FEEDBACK

Email: techdocs@fortinet.com



June 25, 2021

FortiSwitchOS 6.2.5 Administration Guide—Standalone Mode

TABLE OF CONTENTS

Change log	12
Introduction	13
Supported models.....	13
What's new in FortiSwitchOS 6.2.5.....	13
Feature matrix: FortiSwitchOS 6.2.5.....	14
Before you begin.....	21
How this guide is organized.....	21
Management ports	23
Models without a dedicated management port.....	23
Models with a dedicated management port.....	26
Remote access to the management port.....	28
Example configurations.....	29
Configuring administrator tasks	32
Setting the time and date.....	32
Configuring the temperature sensor.....	33
Upgrading the firmware.....	33
Verifying image integrity.....	35
Restore or upgrade the BIOS.....	35
Setting the boot partition.....	36
Backing up the system configuration.....	36
Remote authentication servers.....	36
RADIUS server.....	37
TACACS+ server.....	38
Configuring system administrators.....	39
Access control.....	41
Setting the idle timeout.....	45
Configuring administrative logins.....	46
Configuring security checks.....	47
Logging.....	49
Syslog server.....	50
Fault relay support.....	51
Using SSH and the Telnet client.....	51
Configuring SNMP	52
SNMP access.....	52

SNMP agent	52
SNMP community	53
Adding an SNMP v1/v2c community	53
Adding an SNMP v3 user	54
Global system and switch settings	55
Configuration file settings	55
SSL configuration	55
Configuration file revisions	56
IP conflict detection	57
Port flap guard	58
Retaining the triggered state	58
Configuring the port flap guard	59
Resetting a port	60
Viewing the port flap guard configuration	60
Link monitor	61
Configuring the link monitor	61
Unicast hashing	62
Cut-through switching mode	62
Enabling packet forwarding	62
ARP timeout value	63
Power over Ethernet configuration	63
Creating a schedule	64
Overlapping subnets	66
Physical port settings	67
Configuring general port settings	67
Viewing port statistics	68
Configuring flow control and priority-based flow control	69
Auto-module speed detection	70
Setting port speed (autonegotiation)	70
Link-layer discovery protocol	71
Configuring power over Ethernet on a port	71
Enabling or disabling PoE in the GUI	71
Configuring PoE in the CLI	71
Determining the PoE power capacity	72
Resetting the PoE power	72
Displaying PoE information	72
Energy-efficient Ethernet	73
Diagnostic monitoring interface module status	73
Configuring split ports	75
Configuring QSFP low-power mode	77
Layer-2 interfaces	78
Switched interfaces	78

Viewing interface configuration.....	78
Dynamic MAC address learning.....	79
Configuring dynamic MAC address learning.....	79
Changing when MAC addresses are deleted.....	79
Logging dynamic MAC address events.....	80
Using the learning-limit violation log.....	80
Persistent (sticky) MAC addresses.....	81
Static MAC addresses.....	82
Fortinet loop guard.....	82
Configuring loop guard.....	83
Viewing the loop guard configuration.....	83
VLANs and VLAN tagging.....	84
Native VLAN.....	84
Allowed VLAN list.....	84
Untagged VLAN list.....	85
Packet processing.....	85
Ingress port.....	85
Egress port.....	85
Configuring VLANs.....	86
Example 1.....	86
Example 2.....	87
VLAN stacking (QinQ).....	88
Spanning Tree Protocol.....	93
MSTP overview and terminology.....	93
Regions.....	93
IST.....	93
CST.....	94
Hop count and message age.....	94
STP port roles.....	94
STP loop protection.....	94
STP root guard.....	95
STP BPDU guard.....	95
MSTP configuration.....	96
Configuring STP settings.....	96
Configuring an MST instance.....	97
Configuring an STP edge port.....	99
Configuring STP loop protection.....	99
Configuring STP root guard.....	99
Configuring STP BPDU guard.....	100
Interactions outside of the MSTP region.....	101
Viewing the MSTP configuration.....	102
Support for interoperability with per-VLAN RSTP (rapid PVST+ or RPVST+).....	102

Configuring rapid PVST or RPVST+ interoperation support	102
Viewing the configuration.....	103
Link aggregation groups.....	104
Configuring the trunk and LAG ports.....	104
Example configuration.....	105
Checking the trunk configuration.....	106
MCLAG.....	107
Notes.....	107
Example configuration.....	108
Viewing the configured trunk.....	109
Configuring an MCLAG with IGMP snooping.....	109
Multi-stage load balance.....	110
Configuring the trunk ports.....	111
Heartbeats.....	111
Configuring heartbeats.....	111
LLDP-MED.....	113
Configuration notes.....	113
LLDP global settings.....	114
Setting the asset tag.....	115
Configuring the location table.....	115
Configuring LLDP profiles.....	116
Configuring an LLDP profile for the port.....	119
Enabling LLDP on a port.....	120
Checking the LLDP configuration.....	121
Configuration deployment example.....	121
Checking LLDP details.....	123
LLDP OIDs.....	123
MAC/IP/protocol-based VLANs.....	125
Overview.....	125
MAC based.....	125
IP based.....	125
Protocol based.....	125
Configuring MAC/IP/protocol-based VLANs.....	125
Example configuration.....	127
Checking the configuration.....	128
Mirroring.....	129
Configuring a SPAN mirror.....	130
Multiple mirror destination ports (MTPs).....	132
Configuring an RSPAN mirror.....	133
Configuring an ERSPAN mirror.....	134
Access control lists.....	139

ACL policy attributes.....	139
Configuring an ACL policy.....	140
Creating or customizing a service.....	142
Creating a policer.....	142
Viewing counters.....	142
Clearing counters.....	143
Clearing unused classifiers.....	143
Configuration examples.....	143
Storm control.....	146
Configuring system-wide storm control.....	146
Configuring port-level storm control.....	147
Displaying the storm-control configuration.....	147
DHCP snooping.....	148
Configuring DHCP snooping.....	148
Set the system-wide DHCP snooping options.....	149
Configure the VLAN settings.....	149
Configure the interface settings.....	150
Checking the DHCP snooping configuration.....	152
Removing an entry from the DHCP snooping binding database.....	153
IP source guard.....	154
Configuring IP source guard.....	154
Enable IP source guard.....	154
Configure IP source guard static entries.....	155
Check the IP source guard entries.....	155
Dynamic ARP inspection.....	156
Configuring DAI.....	156
Checking ARP packets.....	157
IGMP snooping.....	158
Notes.....	158
Configuring IGMP snooping.....	159
Configuring the IGMP querier.....	163
Configuring mRouter ports.....	163
IPv6 router advertisement guard.....	164
Configuring IPv6 RA guard.....	164
Create an IPv6 access list.....	164
Create an IPv6 prefix list.....	165
Create an IPv6 RA-guard policy.....	165
Apply the IPv6 RA-guard policy.....	166
View available IPv6 RA-guard policies.....	167
Private VLANs.....	168
Creating and enabling a PVLAN.....	168

Configuring the PVLAN ports.....	169
Private VLAN example.....	169
Quality of service.....	171
Classification.....	171
Marking.....	172
Queuing.....	172
Determining the egress queue.....	173
Packets with DSCP and CoS values.....	173
Packets with a CoS value but no DSCP value.....	173
Packets with a DSCP value but no CoS value.....	173
Configuring FortiSwitch QoS.....	173
Configure an 802.1p map.....	174
Configure a DSCP map.....	175
Configure the QoS egress policy.....	176
Configure the egress drop mode.....	176
Configure the switch ports.....	177
Configure QoS on trunks.....	178
Configure QoS on VLANs.....	178
Configure CoS and DSCP markings.....	179
Checking the QoS statistics.....	179
Clearing and restoring QoS statistics.....	183
sFlow.....	184
About sFlow.....	184
Configuring sFlow.....	184
Checking the sFlow configuration.....	186
Feature licensing.....	187
About licenses.....	187
Configuring licenses.....	187
Layer-3 interfaces.....	189
Loopback interfaces.....	189
Configuring loopback interfaces.....	189
Switched virtual interfaces.....	190
Configuring a switched virtual interface.....	190
Example SVI configuration.....	190
Viewing the SVI configuration.....	191
Layer-3 routing in hardware.....	191
Router activity.....	191
Equal cost multi-path (ECMP) routing.....	192
Configuring ECMP.....	192
Example ECMP configuration.....	192
Viewing ECMP configuration.....	194
Bidirectional forwarding detection.....	194

Configuring BFD.....	194
Viewing BFD configuration.....	195
Unicast reverse-path forwarding (uRPF).....	195
Configuring uRPF.....	195
IP-MAC binding.....	195
Configuring IP-MAC binding.....	196
Viewing IP-MAC binding configuration.....	197
DHCP server and relay.....	198
Configuring a DHCP server.....	198
Configuring the IP address range.....	200
Assigning IP settings to specific MAC addresses.....	200
Configuring DHCP custom options.....	200
Excluding addresses in DHCP.....	201
Listing DHCP leases.....	201
Breaking DHCP leases.....	201
Detailed operation of a DHCP relay.....	201
Configuring a DHCP relay.....	202
OSPF routing.....	203
Terminology.....	203
How OSPF works.....	204
Configuring OSPF.....	205
Check the OSPF configuration.....	207
Example configuration.....	208
RIP routing.....	211
Terminology.....	211
Configuring RIP routing.....	212
Checking the RIP configuration.....	220
Example configuration.....	221
VRRP.....	224
Configuring VRRP.....	224
Checking the VRRP configuration.....	225
BGP routing.....	226
Terminology.....	226
Configuring BGP.....	226
Other BGP commands.....	227
Sample configurations.....	228
Configure system interfaces.....	228
Internal BGP.....	229
External BGP.....	230
PIM routing.....	232
Terminology.....	232
Configuring PIM.....	232

Checking the PIM configuration.....	233
IS-IS routing.....	234
Terminology.....	234
Configuring IS-IS.....	234
Configuring BFD for IS-IS.....	235
Checking the IS-IS configuration.....	235
Users and user groups.....	236
Users.....	236
User groups.....	237
802.1x authentication.....	239
Dynamic VLAN assignment.....	240
MAC authentication bypass (MAB).....	241
Configuring global settings.....	243
Configuring the 802.1x settings on an interface.....	245
Viewing the 802.1x details.....	249
Using the monitor mode.....	251
Clearing port authorizations.....	251
Authenticating users with a RADIUS server.....	252
Example: RADIUS user group.....	255
Example: dynamic VLAN.....	258
Authenticating an admin user with RADIUS.....	258
RADIUS accounting and FortiGate RADIUS single sign-on.....	261
Configuring the RADIUS accounting server and FortiGate RADIUS single sign-on.....	262
Example: RADIUS accounting and single sign-on.....	263
RADIUS change of authorization (CoA).....	263
Configuring CoA and disconnect messages.....	264
Example: RADIUS CoA.....	265
Viewing the CoA configuration.....	266
Use cases.....	266
Use case 1.....	266
Use case 2.....	267
Use case 3.....	268
Detailed deployment notes.....	269
TACACS.....	270
Administrative accounts.....	270
Configuring a TACACS admin account.....	270
User accounts.....	271
Configuring a user account.....	271
Configuring a user group.....	271
Example configuration.....	271
Troubleshooting and support.....	273
Dashboard.....	273

Operation mode.....	273
FortiSwitch Cloud.....	274
Bandwidth.....	275
Losses.....	276
Virtual wire.....	276
TFTP network port.....	277
Cable diagnostics.....	277
Selective packet sampling.....	278
Packet capture.....	279
Create a packet-capture profile.....	280
Start the packet capture.....	280
Pause or stop the packet capture.....	280
Display or upload the packet capture.....	281
Delete the packet-capture file.....	281
Network monitoring.....	281
Directed mode.....	281
Survey mode.....	283
Network monitoring statistics.....	283
Flow tracking and export.....	284
Enabling packet sampling.....	284
Configuring flow export.....	285
Viewing the flow-export data.....	287
Deleting the flow-export data.....	287
Identifying a specific FortiSwitch unit.....	287
Deployment scenario.....	288
Working configuration for PC and phone for 802.1x authentication using MAC.....	288
Summary.....	288
A. Configure all devices.....	288
B. Authenticate phone using MAB.....	292
C. Authenticate the PC using EAP dot1x.....	294
Appendix: FortiSwitch-supported RFCs.....	296
Appendix: Supported attributes for RADIUS CoA and RSSO.....	302

Change log

Date	Change Description
September 14, 2020	Initial release for FortiSwitchOS 6.2.5
January 4, 2021	Added a note to the beginning of the “Mirroring” section.
January 27, 2021	Added the “Configuring rapid PVST or RPVST+ interoperation” section.
January 28, 2021	Updated the “Configuring rapid PVST or RPVST+ interoperation support” section.
June 25, 2021	Updated the “Checking ARP packets” and “Configure the OSPF router” sections.

Introduction

This guide provides information about configuring a FortiSwitch unit in standalone mode. In standalone mode, you manage the FortiSwitch unit by connecting directly to the unit, either using the web-based manager (also known as the GUI) or the CLI.

If you will be managing your FortiSwitch unit using a FortiGate unit, refer to the following guide: [FortiSwitch Managed by FortiOS 6.2](#).

This chapter covers the following topics:

- [Supported models on page 13](#)
- [What's new in FortiSwitchOS 6.2.5 on page 13](#)
- [Feature matrix: FortiSwitchOS 6.2.5 on page 14](#)
- [Before you begin on page 21](#)
- [How this guide is organized on page 21](#)

Supported models

This guide is for all FortiSwitch models that are supported by FortiSwitchOS, which includes all of the D-series and E-series models.

What's new in FortiSwitchOS 6.2.5

FortiSwitch 6.2.5 is a patch release only. No new features or enhancements have been implemented in this release.

Refer to [Feature matrix: FortiSwitchOS 6.2.5 on page 14](#) for details about the features supported on each FortiSwitch model.

Feature matrix: FortiSwitchOS 6.2.5

The following table lists the FortiSwitch features in Release 6.2.5 that are supported on each series of FortiSwitch models. All features are available in Release 6.2.5, unless otherwise stated.

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Management and Configuration									
CPLD software upgrade support for OS	—	—	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support)	—	✓	✓	148E 148E-POE	✓	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓	✓	✓
Support for switch SNMP OID	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP conflict detection and notification	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiSwitch Cloud configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security and Visibility									
802.1x port mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x enhancements, including MAB	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MAB reauthentication disabled	—	✓	✓	✓	✓	✓	✓	✓	✓
open-auth mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
Support of the RADIUS accounting server	Partial	✓	✓	✓	✓	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages	—	✓	✓	✓	✓	✓	✓	✓	✓
EAP Pass-Through	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network device detection	—	—	✓	—	✓	✓	✓	✓	✓
IP-MAC binding	✓	—	—	—	—	—	✓	✓	✓
sFlow	✓	✓	✓	—	✓	✓	✓	✓	✓
Flow export	—	—	✓	—	✓	✓	✓	✓	✓
ACL	—	—	✓	—	✓	✓	✓	✓	✓
Multistage ACL	—	—	—	—	—	—	✓	✓	✓
Multiple ingress ACLs	—	—	✓	—	✓	✓	✓	✓	✓
Schedule for ACLs	—	—	✓	—	✓	✓	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
Allowed DHCP server list	—	✓	✓	✓	✓	✓	✓	✓	✓
DHCP blocking	—	—	✓	—	✓	✓	✓	✓	✓
IP source guard	—	—	✓	—	✓	✓	—	—	—
Dynamic ARP inspection	✓	—	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓	✓
Access VLANs	—	✓	✓	✓	✓	✓	✓	✓	✓
VLAN tag by ACL	—	—	✓	—	✓	✓	✓	✓	✓
RMON group 1	—	✓	✓	✓	✓	✓	✓	✓	✓
Reliable syslog (RFC 6587)	—	✓	✓	✓	✓	✓	✓	✓	✓
Packet capture	—	—	✓	—	✓	✓	✓	✓	✓
Layer 2									
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	8	8	24/48	24/48	24/64
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 RA guard	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP proxy	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP querier	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED: ELIN support	—	✓	✓	✓	✓	✓	✓	✓	✓
LLPD-MED: PoE negotiation	—	✓	✓	✓	✓	✓	✓	—	—
Per-port max for learned MACs	—	—	✓	✓	✓	✓	✓	—	—
MAC learning limit (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Learning limit violation log (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
set mac-violation-timer	—	✓	✓	✓	✓	✓	✓	✓	✓
Sticky MAC	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total MAC entries	—	✓	✓	✓	✓	✓	✓	✓	✓
MSTP instances	—	0-15	0-15	0-15	0-15	0-15	0-32	0-32	0-32
STP root guard	—	✓	✓	✓	✓	✓	✓	✓	✓
STP BPDU guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid PVST interoperation	—	✓	✓	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces	—	✓	✓	✓	✓	✓	✓	✓	✓
Private VLANs	✓	—	✓	—	✓	✓	✓	✓	✓
Multi-stage load balancing	—	—	—	—	—	—	—	✓	✓
Priority-based flow control	—	—	—	—	—	—	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per-port storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	—	✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Percentage rate control	✓	—	✓	—	✓	✓	✓	✓	✓
VLAN stacking (QinQ)	—	—	✓	—	✓	✓	✓	✓	✓
VLAN mapping	—	—	✓	—	✓	✓	✓	✓	✓
SPAN	✓	✓	✓	✓	✓	✓	✓	✓	✓
RSPAN and ERSPAN	—	RSPAN	✓	—	✓	✓	✓	✓	✓
Layer 3									
Static routing (v4 v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Hardware routing offload (v4 v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Software routing only	✓	✓	—	✓	—	—	—	—	—
OSPF (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
RIP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
VRRP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
BGP (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
IS-IS (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
PIM (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
Hardware-based ECMP	—	—	—	—	—	—	✓	✓	✓
Static BFD	—	—	✓	✓	✓	✓	✓	✓	✓
uRPF	—	—	—	—	—	—	✓	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
DHCP server	—	—	—	—	✓	4xx only	✓	✓	✓
High Availability									
MCLAG (multichassis link aggregation)	Partial	—	—	—	✓	✓	✓	✓	✓
STP supported in MCLAGs	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping support in MCLAG	✓	—	—	—	✓	✓	✓	✓	✓
Quality of Service									
802.1p support, including priority queuing trunk and WRED	✓	—	✓	—	✓	✓	✓	✓	✓
QoS queue counters	—	—	✓	—	✓	✓	✓	✓	✓
QoS marking	—	—	✓	—	✓	✓	✓	✓	✓
Summary of configured queue mappings	✓	—	✓	✓	✓	✓	✓	✓	✓
Egress priority tagging	—	—	✓	—	✓	✓	✓	✓	✓
Miscellaneous									
PoE-pre-standard detection (See Note 1.)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—
PoE modes support: first come, first served or priority based (PoE models)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Control of temperature alerts	—	✓	✓	—	✓	✓	✓	✓	✓
Split port (See Note 6.)	Partial	—	—	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support	✓	—	✓	—	✓	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support)	—	✓	✓	—	✓	✓	✓	✓	✓
Cut-through switching	—	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode	—	—	—	—	—	—	✓	1048D 1048E	✓
Energy-efficient Ethernet	—	✓	✓	✓	✓	✓	✓	—	—
PHY Forward Error Correction (see Note 5)	—	—	—	—	—	—	—	1048E	3032E

Notes

- PoE features are applicable only to the model numbers with a POE or FPOE suffix.
- 24-port LAG is applicable to 524D, 524-FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
- To use the dynamic layer-3 protocols, you must have an advanced features license.
- The per-VLAN MAC learning limit and per-trunk MAC learning limit are not supported on the 448D/448D-POE/448D-FPOE/248E-POE/248E-FPOE/248D series.

5. Supported only in 100G mode (clause 91).
6. On the 3032E, you can split one port at the full base speed, split one port into four sub-ports of 25 Gbps each (100G QSFP only), or split one port into four sub-ports of 10 Gbps each (40G or 100G QSFP).

Before you begin

Before you start administrating your FortiSwitch unit, it is assumed that you have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch model and have administrative access to the FortiSwitch unit's GUI and CLI.

How this guide is organized

This guide is organized into the following chapters:

- [Management ports](#) describes how to configure the management ports.
- [Configuring administrator tasks](#) describes how to configure the date and time, admin users, and remote authentication servers.
- [Configuring SNMP](#) describes how to monitor hardware on your network.
- [Global system and switch settings](#) describes the initial configuration of your FortiSwitch unit.
- [Physical port settings](#) describes how to configure the physical ports.
- [Layer-2 interfaces](#) describes how to configure layer-2 interfaces.
- [VLANs and VLAN tagging](#) describes how to configure VLANs and describes the packet flow for VLAN tagged and untagged packets.
- [Spanning Tree Protocol](#) describes how to configure MSTP.
- [Link aggregation groups](#) describes how to configure link aggregation groups.
- [MCLAG](#) describes how to configure MCLAG.
- [Multi-stage load balance](#) describes how to configure multi-stage load balancing on a set of FortiGate units.
- [LLDP-MED](#) describes how to configure LLDP-MED settings.
- [MAC/IP/protocol-based VLANs](#) describes how to configure MAC/IP/protocol-based VLANs.
- [Mirroring](#) describes how to configure port mirroring.
- [Access control lists](#) describes how to configure ACLs.
- [Storm control](#) describes how to configure storm control.
- [DHCP snooping](#) describes how to configure DHCP snooping.
- [IP source guard](#) describes how to configure IP source guard.
- [Dynamic ARP inspection](#) describes how to configure dynamic ARP inspection.
- [IGMP snooping](#) describes how to configure IGMP snooping.
- [Private VLANs](#) describes how to create and manage private virtual local area networks (VLANs).
- [Quality of service](#) describes how to configure QoS.
- [sFlow](#) describes how to configure sFlow.
- [Feature licensing](#) describes feature licenses.
- [Layer-3 interfaces](#) describes how to configure routed ports, routed VLAN interfaces, switch virtual interfaces, and related features.

- [DHCP server and relay](#) describes how to configure DHCP servers and relays.
- [OSPF routing](#) describes how to configure OSPF routing.
- [RIP routing](#) describes how to configure RIP routing.
- [VRRP](#) describes how to configure VRRP.
- [BGP routing](#) describes how to configure BGP routing.
- [PIM routing](#) describes how to configure PIM routing.
- [IS-IS routing](#) describes how to configure IS-IS routing.
- [Users and user groups](#) describes how to configure users and user groups.
- [802.1x authentication](#) describes how to configure 802.1x authentication (to RADIUS servers).
- [TACACS](#) describes how to configure TACACS authentication.
- [Troubleshooting and support](#) describes ways to gather more details and to solve problems.
- [Deployment scenario](#) describes an example configuration.
- [Appendix: FortiSwitch-supported RFCs](#) lists RFCs that are supported by FortiSwitchOS.

Management ports

This chapter describes how to configure management ports on the FortiSwitch unit.

The following topics are covered:

- [Models without a dedicated management port on page 23](#)
- [Models with a dedicated management port on page 26](#)
- [Remote access to the management port on page 28](#)
- [Example configurations on page 29](#)

Models without a dedicated management port

For FortiSwitch models without a dedicated management port, configure the internal interface as the management port.

NOTE: For FortiSwitch models without a dedicated management port, the internal interface has a default VLAN ID of 1.

Using the GUI:

First start by editing the default *internal* interface's configuration.

1. Go to *System > Network > Interface > Physical*, select *Edit* for the *internal* interface.

Edit Physical Interface

Name	internal
MAC Address	08:5b:0e:f1:95:e5
Alias	<input type="text"/>

IP Configuration

Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP/Netmask	<input type="text" value="0.0.0.0/0.0.0.0"/>

Administration

Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> RADIUS Accounting <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP
--------	--

Secondary IP

ID(1-65535)	Address	Access	Manage
+Add IP			

DHCP Relay

Enabled	<input type="checkbox"/>
---------	--------------------------

VRRP

Virtual MAC	<input type="checkbox"/>
-------------	--------------------------

Status	ID (1-255)	Group (1-65535)	Priority (1-255)	Preempt	Source IP	Destination(s)	Manage
+Add VRRP							
							Cancel Update

- In the IP/Netmask field, enter the IP address and netmask.
- Select the appropriate protocols to connect to the interface for administrative access.
- Optional. Select *Add IP* to add a secondary IP address for the internal interface.
- Select *Update* to save your changes.

Next, create a new interface to be used for management.

- Go to *System > Network > Interface > VLAN* and select *Add VLAN* to create a management VLAN.

Add VLAN Interface

Name

Alias

Interface

VLAN ID (1-4093)

IP Configuration

Mode Static
 DHCP

IP/Netmask

Administration

Status Up
 Down

Access HTTPS
 HTTP
 PING
 RADIUS Accounting
 SSH
 TELNET
 SNMP

Secondary IP

ID(1-65535)	Address	Access	Manage
+Add IP			

DHCP Relay

Enabled

VRRP

Status	ID (1-255)	Group (1-65535)	Priority (1-255)	Preempt	Source IP	Destination(s)	Manage
+Add VRRP							

[Cancel](#) [Add](#)

2. Give the interface an appropriate name.
3. Confirm that *Interface* is set to *internal*.
4. Set a *VLAN ID*.
5. In the IP/Netmask field, enter the IP address and netmask.
6. Select the appropriate protocols to connect to the interface for administrative access.
7. Optional. Select *Add IP* to add a secondary IP address for this VLAN.
8. Select *Add*.

Using the CLI:

```

config system interface
  edit internal
    set ip <IP_address_and_netmask>
    set allowaccess <access_types>
    set type physical
    set secondary-IP enable
    config secondaryip
      edit <id>
        set ip <IP_address_and_netmask>
        set allowaccess <access_types>
      next
    end
  end

```

```
next
edit <vlan name>
  set ip <IP_address_and_netmask>
  set allowaccess <access_types>
  set interface internal
  set vlanid <VLAN id>
  set secondary-IP enable
  config secondaryip
    edit <id>
      set ip <IP_address_and_netmask>
      set allowaccess <access_types>
    end
  end
end
```

Models with a dedicated management port

For FortiSwitch models with a dedicated management port, configure the IP address and allowed access types for the management port.

NOTE: For FortiSwitch models with a dedicated management port, the internal interface has a default VLAN identifier of 4094.

Using the GUI:

1. Go to *System > Network > Interface > Physical*, select *Edit* for the *mgmt* interface.

Edit Physical Interface

Name: mgmt
 MAC Address: 08:5b:0e:f1:95:e4
 Alias:

IP Configuration

Mode: Static DHCP
 Distance: (1-255)
 Retrieve Default Gateway from Server:
 Override Internal DNS:

Administration

Access: HTTPS HTTP PING RADIUS Accounting SSH TELNET SNMP

Secondary IP

ID(1-65535)	Address	Access	Manage
<input type="text" value="1"/>	<input type="text" value="192.168.1.99 255.255.255.0"/>	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> RADIUS Accounting <input type="checkbox"/> SSH <input type="checkbox"/> TELNET <input type="checkbox"/> SNMP	<input type="button" value="Remove"/> <input type="button" value="+ Add IP"/>

DHCP Relay

Enabled:

VRRP

Virtual MAC:

Status	ID (1-255)	Group (1-65535)	Priority (1-255)	Preempt	Source IP	Destination(s)	Manage
							<input type="button" value="+ Add VRRP"/> <input type="button" value="Cancel"/> <input type="button" value="Update"/>

2. In the ID field, enter a unique identifier from 1 to 65525.
3. In the *IP/Netmask* field, enter the IP address and netmask.
4. Select the appropriate protocols to connect to the interface for administrative access.
5. Optional. You can select *Remove* if you want to delete the default secondary IP address or select *Add IP* to add a secondary IP address for the management interface.
6. Select *Update* to save your changes.

Using the CLI:

```

config system interface
  edit mgmt
    set ip <IP_address_and_netmask>
    set allowaccess <access_types>
    set type physical
    set secondary-IP enable
    config secondaryip
      edit <id>
        set ip <IP_address_and_netmask>
        set allowaccess <access_types>
      next
    end
  next
end

```

```
edit internal
  set type physical
end
end
```

Remote access to the management port

To provide remote access to the management port, configure a static route. Set the gateway address to the IP address of the router.

Using the GUI:

1. Go to *Router > Config > Static* and select *Add Route*.

Add Static Route

ID	<input type="text"/>	(1-2147483647)
	This value is required.	
Status	<input checked="" type="checkbox"/>	
Destination IP/Netmask	<input type="text" value="0.0.0.0 0.0.0.0"/>	
Blackhole	<input type="checkbox"/>	
Device	<input type="text" value="Any"/>	
Gateway	<input type="text"/>	
	This value is required.	
Dynamic Gateway	<input type="checkbox"/>	
Comments	<input type="text"/>	
	<input type="button" value="Cancel"/>	<input type="button" value="Add"/>

2. Enter an identifier. This is a unique number to identify the static route.
3. Select the Status checkbox if it is not selected.
4. Set the device to *mgmt*.
5. Set the gateway to the gateway router IP address.
6. Select *Add*.

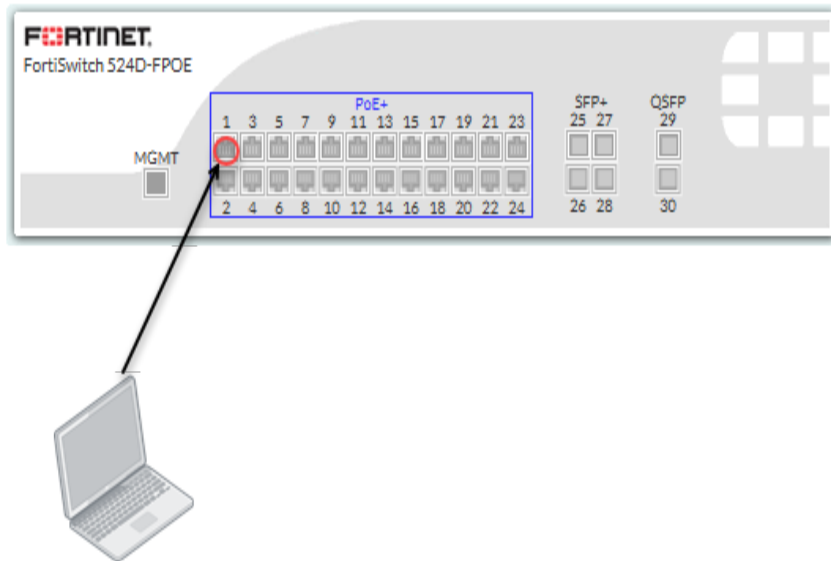
Using the CLI:

```
config router static
  edit 1
    set device mgmt
    set gateway <router IP address>
    set status enable
  end
end
```

Example configurations

In this example, the *internal* interface is used as an inbound management interface. Also, the FortiSwitch unit has a default VLAN across all physical ports and its internal port.

Using the internal interface of a FortiSwitch-524D-FPOE

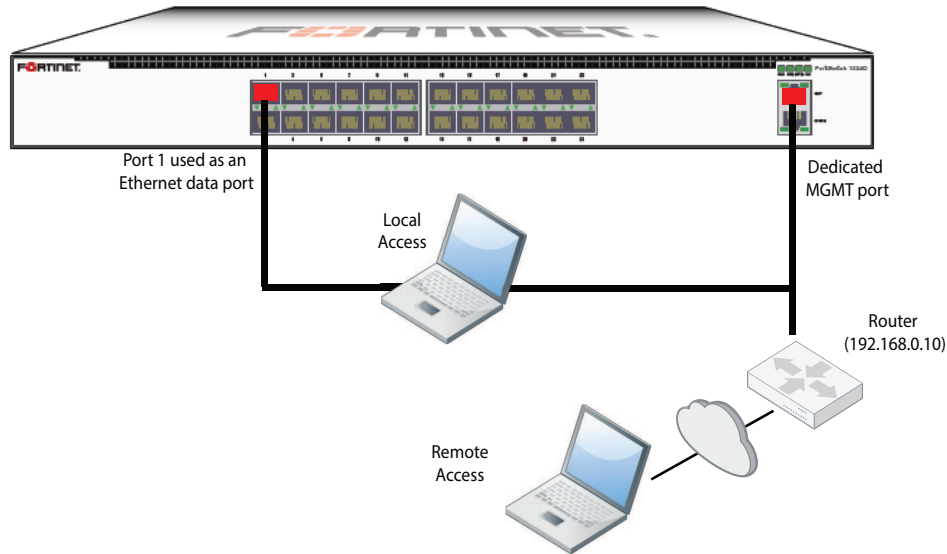


Syntax

```
config system interface
  edit internal
    set ip 192.168.1.99 255.255.255.0
    set allowaccess ping https http ssh
    set type physical
  end
end
```

In this example, an out-of-band management interface is used as the dedicated management port. You can configure the management port for local or remote access.

Out-of-band management on a FortiSwitch-1024D



Option 1: management port with static IP

```

config system interface
  edit mgmt
    set mode static
    set ip 10.105.142.19 255.255.255.0
    set allowaccess ping https http ssh snmp telnet
    set type physical
  next
  edit internal
    set type physical
  end
end
// optional configuration to allow remote access to the management port

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

```

Option 2: management port with IP assigned by DHCP

```

config system interface
  edit mgmt
    set mode dhcp
    set defaultgw enable // allows remote access
    set allowaccess ping https http ssh snmp telnet

```

```
    set type physical
next
edit internal
    set type physical
end
```

Configuring administrator tasks

You can use the default “admin” account to configure administrator accounts, adjust system settings, upgrade firmware, create backup files, and configure security features.

This chapter covers the following topics:

- [Setting the time and date on page 32](#)
- [Configuring the temperature sensor on page 33](#)
- [Setting the boot partition on page 36](#)
- [Upgrading the firmware on page 33](#)
- [Backing up the system configuration on page 36](#)
- [Remote authentication servers on page 36](#)
- [Configuring system administrators on page 39](#)
- [Configuring administrative logins on page 46](#)
- [Configuring security checks on page 47](#)
- [Logging on page 49](#)
- [Fault relay support on page 51](#)
- [Using SSH and the Telnet client on page 51](#)

Setting the time and date

For effective scheduling and logging, the system date and time must be accurate. You can either manually set the system date and time or configure the system to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

NOTE: Some FortiSwitch models do not have a battery-backup real-time clock. For FortiSwitch models without a real-time clock, the time is reset when the switch is rebooted. These models must be connected to an NTP server if you want to maintain the correct system date and time.

The Network Time Protocol enables you to keep the system time synchronized with other network systems. This will also ensure that logs and other time-sensitive settings are correct.

To set the date and time:

1. Go to *System > Dashboard*.
2. Next to the *System Time* field, select *Change*.

Dashboard

System Information			
Serial Number	S548DF5018000776	System Configuration	Last Backup: Never [Backup] [Restore] [Revisions]
BIOS Version	04000018	System Time	Thu Apr 4th 2019 02:19:34 PM [Change]
Firmware Version	v6.2.0,build0167.190404 (Interim) [Upgrade]	Uptime	0 Day, 0 Hour, 12 Minutes [Reboot] [Shut Down]
Current Administrator	admin [Change Password] / 1 in Total [Details]	Current License	[Change]
Operation Mode	Local Management	FortiSwitchCloud	🟢 Connected

3. Select your *Time Zone*.
4. Either select *Manual Setting* and enter the system date and time or select *Synchronize with NTP Server*. If you select synchronization, you can either use the default FortiGuard server or specify a different server. You can also set the *Sync Interval*.
5. Select *Update*.

If you use an NTP server, you can identify a specific port/IP address for this self-originating traffic. The configuration is performed in the CLI with the command `set source-ip`. For example, you can set the source IP address of NTP to be on the DMZ1 port with an IP of 192.168.4.5:

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

Configuring the temperature sensor

If your FortiSwitch unit has a temperature sensor, you can set a warning and an alarm for when the system temperature reaches specified temperatures. When these thresholds are exceeded, a log message and SNMP trap are generated. The warning threshold must be lower than the alarm threshold.

Use the following commands to set warning and alarm thresholds:

```
config system snmp sysinfo
  set status enable
  set trap-temp-warning-threshold <temperature in degrees Celsius>
  set trap-temp-alarm-threshold <temperature in degrees Celsius>
end
```

By default, the FortiSwitch unit generates an alert (in the form of an SNMP trap and a SYSLOG entry) every 30 minutes when the temperature sensor exceeds its set threshold. You can change this interval with the following commands:

```
config system global
  set alertd-relog enable
  set alert-interval <1-1440 minutes>
end
```

Upgrading the firmware

Use these procedures to upgrade your FortiSwitch firmware.

Using the GUI

You can upgrade the firmware from the dashboard or from the system configuration page.

To upgrade the firmware from the dashboard:

1. Go to *System > Dashboard*.
2. Next to the *Firmware Version* field, select *Update*.

Dashboard

System Information			
Serial Number	S548DF5018000776	System Configuration	Last Backup: Never [Backup] [Restore] [Revisions]
BIOS Version	04000018	System Time	Thu Apr 4th 2019 02:19:34 PM [Change]
Firmware Version	v6.2.0,build0167,190404 (Interim) [Upgrade]	Uptime	0 Day, 0 Hour, 12 Minutes [Reboot] [Shut Down]
Current Administrator	admin [Change Password] / 1 in Total [Details]	Current License	[Change]
Operation Mode	Local Management	FortiSwitchCloud	🟢 Connected

To upgrade the firmware from the system configuration page:

1. Go to *System > Config > Firmware*.
2. Select *Choose File* and then navigate to the firmware image.

Firmware

Current Running Firmware: S524DF-6.0.0-build0013

Memory Usage: Total: 2,074 MB / Free: 1,742 MB / Usable: 1,742 MB

Upgrade File Choose File...

Allow Firmware Downgrade

Apply

3. Select *Apply*.

Using the CLI:

You can download a firmware image from an FTP server, from a FortiManager unit, or from a TFTP server. The FortiSwitch unit reboots and then loads the new firmware.

```
execute restore image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]>[<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
```

The following example shows how to upload a configuration file from a TFTP server to the FortiSwitch unit and restart the FortiSwitch unit 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
```

You can also load a firmware image from an FTP or TFTP server without restarting the FortiSwitch unit:

```
execute stage image ftp <string> <ftp server>[:ftp port]
execute stage image tftp <string> <ip>
```

Verifying image integrity

To verify the integrity of the images in the primary and secondary (if applicable) flash partitions, use the following commands:

```
execute verify image primary
execute verify image secondary
```

If the image is corrupted or missing, the command fails with a return code of `-1`.

For 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
```

Restore or upgrade the BIOS

You can restore or upgrade the basic input/output system (BIOS) if needed. After a BIOS upgrade, passwords for all FortiSwitch local users must be reconfigured using the `config user local` setting.

CAUTION: Only restore or upgrade the BIOS if Customer Support recommends it.

To upgrade or restore the BIOS from the CLI:

```
execute restore bios tftp <filename_str> <server_ipv4[:port_int]>
```

For example:

```
execute restore bios tftp PPC/FS-3032D/04000009/FS3D323Z14000004.bin 10.105.2.201
```

The example downloads the BIOS file from the TFTP server at the specified IPv4 address.

NOTE: If the BIOS upgrade fails, do not restart the FortiSwitch unit. Instead, try the CLI command again. If repeating the CLI command does not work, the FortiSwitch unit might require a return merchandise authorization (RMA).

Setting the boot partition

You can specify the flash partition for the next reboot. The system can use the boot image from either the primary or the secondary flash partition:

```
execute set-next-reboot <primary | secondary>
```

NOTE: You must disable image rotation before you can use the `execute set-next-reboot` command.

If your FortiSwitch model has dual flash memory, you can use the primary and backup partitions for image rotation. By default, this feature is enabled.

```
config system global
  set image-rotation <enable | disable>
end
```

To list all of the flash partitions:


```
diagnose sys flash list
```

Backing up the system configuration

To back up the configuration from the dashboard:

1. Go to *System > Dashboard*.
2. Next to the *System Configuration* field, select *Backup*.
You can enter a password to encrypt the backup file. Passwords can be up to 15 characters in length.

Dashboard

System Information			
Serial Number	SS48DF5018000776	System Configuration	Last Backup: Never [Backup] [Restore] [Revisions]
BIOS Version	04000018	System Time	Thu Apr 4th 2019 02:19:34 PM [Change]
Firmware Version	v6.2.0.build0167.190404 (Interim) [Upgrade]	Uptime	0 Day, 0 Hour, 12 Minutes [Reboot] [Shut Down]
Current Administrator	admin [Change Password] / 1 in Total [Details]	Current License	[Change]
Operation Mode	Local Management	FortiSwitchCloud	 Connected

Remote authentication servers

If you are using remote authentication for administrators or users, you need to configure one of the following:

- RADIUS server
- TACACS+ server

RADIUS server

The information you need to configure the system to use a RADIUS server includes:

- the RADIUS server's domain name or IP address
- the RADIUS server's shared secret key



The default port for RADIUS traffic is 1812. Some RADIUS servers use port 1645. You can configure the FortiSwitch unit to use port 1645:

```
config system global
  set radius-port 1645
end
```

To configure RADIUS authentication with the GUI:

1. Go to *System > Authentication > RADIUS* and select *Add Server*.

Add RADIUS Server

Name	<input type="text"/>
Primary Server Address	<input type="text"/>
Primary Server Secret	<input type="text"/> 
Secondary Server Name/IP	<input type="text"/>
Secondary Server Secret	<input type="text"/> 
Authentication Scheme	<input checked="" type="radio"/> Use Default Authentication Scheme <input type="radio"/> Specify Authentication Protocol
NAS IP/Called Station ID	<input type="text"/>
Include in every User Group	<input type="checkbox"/>

2. Enter the following information and select *Add*.

Field	Description
Name	Enter a name to identify the RADIUS server on the FortiSwitch unit.
Primary Server Address	Enter the domain name (such as fgt.example.com) or the IP address of the RADIUS server.

Field	Description
Primary Server Secret	<p>Enter the server secret key, such as radiusSecret. This key can be a maximum of 16 characters long.</p> <p>This value must match the secret on the RADIUS primary server.</p>
Secondary Server Name/IP	<p>Optionally enter the domain name (such as fgt.example.com) or the IP address of the secondary RADIUS server.</p>
Secondary Server Secret	<p>Optionally, enter the secondary server secret key, such as radiusSecret2. This key can be a maximum of 16 characters long.</p> <p>This value must match the secret on the RADIUS secondary server.</p>
Authentication Scheme	<p>If you know the RADIUS server uses a specific authentication protocol, select <i>Specify Authentication Protocol</i> and select the protocol from the list. Otherwise, select <i>Use Default Authentication Scheme</i>. The default authentication scheme will usually work.</p>
NAS IP/Called Station ID	<p>Enter the IP address to be used as an attribute in RADIUS access requests.</p> <p>The NAS IP address is a RADIUS setting or IP address of the FortiSwitch interface used to talk to the RADIUS server, if not configured.</p> <p>The Called Station ID is the same value as the NAS IP address but in text format.</p>
Include in every User Group	<p>When this option is enabled, this RADIUS server is automatically included in all user groups. This option is useful if all users will be authenticating with the remote RADIUS server.</p>

To configure the FortiSwitch unit for RADIUS authentication, see [802.1x authentication on page 239](#).

TACACS+ server

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices using one or more centralized servers. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

TACACS+ offers fully encrypted packet bodies and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP protocol.

To configure TACACS+ authentication using the GUI:

1. Go to *System > Authentication > TACACS* and select *Add Server*.

Add TACACS Server

Name

Server Address

Server Key

Authentication Type Auto ▼

2. Enter the following information and select *Add*.

Field	Description
Name	Enter a name to identify the TACACS server on the FortiSwitch unit.
Server Address	Enter the domain name (such as fgt.example.com) or the IP address of the TACACS server.
Server Key	Enter the server key for the TACACS server.
Authentication Type	Select the authentication type to use for the TACACS+ server. <i>Auto</i> tries PAP, MSCHAP, and CHAP (in that order).

To configure the FortiSwitch unit for TACACS+ authentication, see [TACACS on page 270](#).

Configuring system administrators

In addition to the default “admin” account, you might want to set up other administrators with different levels of system access.

This section covers the following topics:

- [Administrator profiles on page 40](#)
- [Creating administrator profiles on page 40](#)
- [Access control on page 41](#)
- [Adding administrators on page 43](#)
- [Monitoring administrators on page 44](#)
- [Setting the default administrator password on page 45](#)

- [Setting the password retries and lockout time on page 45](#)
- [Setting the idle timeout on page 45](#)

Administrator profiles

Administer profiles define what the administrator user can do when logged into the FortiSwitch unit. When you set up an administrator user account, you also assign an administrator profile, which dictates what the administrator user will see. Depending on the nature of the administrator's work, access level, or seniority, you can allow them to view and configure as much, or as little, as required.

The `super_admin` administrator is the administrative account that the primary administrator should have to log into the FortiSwitch unit. The profile cannot be deleted or modified to ensure there is always a method to administer the FortiSwitch unit. This user profile has access to all components of the system, including the ability to add and remove other system administrators. For some administrative functions, such as backing up and restoring the configuration using SCP, `super_admin` access is required.

Creating administrator profiles

To configure administrator profiles, go to *System > Admin > Profiles*. You can only assign one profile to each administrator user.

On the *Add Profile* page, you define the components of the FortiSwitch unit that will be available to view and/or edit. For example, if you configure a profile so that the administrator can only access System Configuration, this admin will not be able to change Network settings. For more detail about what is covered by each access control, see [Access control on page 41](#).

Using the GUI:

1. Go to *System > Admin > Profiles* and select *Add Profile*.

Add Profile

Profile Name

This value is required.

Access Control	None ↓	Read Only ↓	Read-Write ↓
System Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Admin Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Router Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Log & Report	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Cancel
Add

2. Give the profile an appropriate name.
3. Set *Access Control* as required, selecting *None*, *Read Only*, or *Read-Write* for each line.
4. Select *Add*.

Using the CLI:

```

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

```

Access control

The *System Configuration* access control applies to the following menus:

- *System > Dashboard*
- *System > Network > DNS*
- *System > Network > Settings*
- *System > Config > SNMP > Communities*
- *System > Config > SNMP > Users*
- *System > Config > SNMP > Settings*
- *System > Config > Firmware*

- *System > Config > Backup*
- *System > Config > Revisions*
- *System > Config > Licenses*
- *System > Config > Time*
- *System > Config > SSL*
- *System > User > Definition*
- *System > User > Group*
- *System > Authentication > LDAP*
- *System > Authentication > RADIUS*
- *System > Authentication > TACACS*
- *System > Certificate > Local*
- *System > Certificate > Remote*
- *System > Certificate > Authorities*
- *System > Certificate > CRLs*

The *Network Configuration* access control applies to the follow menus:

- *System > Network > Interface > Physical*
- *System > Network > Interface > VLAN*
- *System > Network > Interface > Loopback*
- *Switch > Port > Physical*
- *Switch > Port > Trunk*
- *Switch > Interface > Physical*
- *Switch > Interface > Trunk*
- *Switch > Interface > Port Security*
- *Switch > STP > Settings*
- *Switch > STP > Instances*
- *Switch > Flap Guard*
- *Switch > LLDP-MED > Profiles*
- *Switch > LLDP-MED > Settings*
- *Switch > POE*
- *Switch > sFlow*
- *Switch > Mirror*
- *Switch > VLAN*
- *Switch > Virtual Wires*
- *Switch > Storm Control*
- *Switch > MAC Entries*
- *Switch > IP-MAC Binding*
- *Switch > QoS > 802.1p*
- *Switch > QoS > IP/DSCP*
- *Switch > QoS > Egress Policy*
- *Switch > Monitor > Forwarding Table*
- *Switch > Monitor > Port Stats*
- *Switch > Monitor > Spanning Tree*

- *Switch > Monitor > Modules*
- *Switch > Monitor > LLDP*
- *Switch > Monitor > Loop Guard*
- *Switch > Monitor > Flap Guard*
- *Switch > Monitor > 802.1x Status*

The *Admin Users* access control applies to the following menus:

- *System > Admin > Administrators*
- *System > Admin > Profiles*
- *System > Admin > Monitor*
- *System > Admin > Settings*

The *Router Configuration* access control applies to the following menus:

- *Router > Config > OSPF > Settings*
- *Router > Config > OSPF > Areas*
- *Router > Config > OSPF > Networks*
- *Router > Config > OSPF > Interfaces*
- *Router > Config > RIP > Settings*
- *Router > Config > RIP > Distances*
- *Router > Config > RIP > Networks*
- *Router > Config > RIP > Interfaces*
- *Router > Config > Static*
- *Router > Config > Interface*
- *Router > Config > Link Probes*
- *Router > Monitor > Routing*
- *Router > Monitor > Link*

The *Log & Report* access control applies to the follow menus:

- *Log > Event Log > Link*
- *Log > Event Log > POE*
- *Log > Event Log > Spanning Tree*
- *Log > Event Log > Switch*
- *Log > Event Log > Switch Controller*
- *Log > Event Log > System*
- *Log > Event Log > Router*
- *Log > Event Log > User*
- *Log > Config*

Adding administrators

Only the default “admin” account can create a new administrator account. If required, you can add an additional account with read-write access control to add new administrator accounts.

If you log in with an administrator account that does not have the super_admin admin profile, the administrators list will show only the administrators for the current virtual domain.

When adding administrators, you are setting up the administrator's user account. An administrator account comprises an administrator's basic settings as well as their access profile. The access profile is a definition of what the administrator is capable of viewing and editing.

Follow one of these procedures to add an administrator.

Using the GUI:

1. Go to *System > Admin > Administrators*.
2. Select *Add Administrator*.

Add Administrator

Name

This value is required.

Type Regular Remote

Password

Confirm Password

Admin Profile

Restrict this Admin Login from Trusted Hosts Only

3. Enter the administrator name.
4. Select the type of account. If you select *Remote*, the system can reference a RADIUS or TACACS+ server.
5. If you selected *Remote*, select the *User Group* the account will access, whether wildcards are accepted, and whether the access profile group can be overridden.
6. Enter the password for the user. Passwords can be up to 64 characters in length.
7. Select *Add*.

Using the CLI:

```
config system admin
  edit <admin_name>
    set password <password>
    set accprofile <profile_name>
  end
```

Monitoring administrators

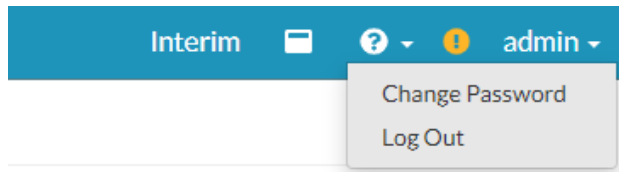
You can find out which administrators are logged in by looking at the *System Information* section of the *Dashboard*. The *Current Administrator* row shows the administrators logged in and the total logged in. Selecting *Details* displays the information for each administrator: where they are logging in from and how and when they logged in.

Setting the default administrator password

By default, your system has an administrator account set up with the user name `admin` and no password. On your first login to the GUI or CLI of a new FortiSwitch unit, you must create a password. You are also forced to create a password after resetting the FortiSwitch configuration to the factory default settings with the `execute factory reset` or `execute factoryresetfull` command.

To change the default password:

1. From the admin menu in the page banner, select *Change Password*.



2. Enter the new password in the *Password* and *Confirm Password* fields. Passwords can be up to 64 characters in length.
3. Select *Change*.

Setting the password retries and lockout time

By default, the system includes a set number of three password retries, allowing the administrator a maximum of three attempts to log into their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts can be set to an alternate value, as well as the default wait time before the administrator can try to enter a password again. You can also change this value to make it more difficult to hack. Both settings are must be configured with the CLI

To configure the lockout options:

```
config system global
  set admin-lockout-threshold <failed_attempts>
  set admin-lockout-duration <seconds>
end
```

For example, to set the lockout threshold to one attempt and the duration before the administrator can try again to log in to five minutes, enter these commands:

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

Setting the idle timeout

By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management PC is left unattended.

To change the idle timeout:

1. Go to *System > Admin > Settings*.
2. Enter the time in minutes in the *Idle Timeout (Minutes)* field.
3. Update other settings as required:
 - TCP/UDP port values for HTTP, HTTPS, Telnet, SSH
 - Display language
4. Select *Apply*.

Configuring administrative logins

You can configure the RADIUS server to set the access profile. This process uses RADIUS vendor-specific attributes (VSAs) passed to the FortiSwitch unit for authorization. The RADIUS access profile override is mainly used for administrative logins.

Using the GUI:

1. Go to *System > Admin > Administrators*.
2. Select *Add Administrator*.
3. Select *Remote*.

Add Administrator

Name
 This value is required.

Type Regular Remote

User Group

Wildcard

Accprofile Override

Backup Password

Confirm Password

Admin Profile

Restrict this Admin Login from Trusted Hosts Only

4. In the Administrator field, enter a name for the RADIUS system administrator.
5. Select the user group.
6. Select *Wildcard*.
7. Select *Accprofile Override*.
8. Select *Add*.

Using the CLI:

The following code creates a RADIUS-system admin group with accprofile-override enabled:

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

Ensure that the RADIUS server is configured to send the appropriate VSA.

To send an appropriate group membership and access profile, set VSA 1 and VSA 6, as in the following code:

```
VENDOR fortinet 12356
ATTRIBUTE Fortinet-Group-Name 1 <admin profile>
ATTRIBUTE Fortinet-Access-Profile 6 <access profile>
```

The value of VSA 1 must match the remote group, and VSA 6 must match a valid access profile.

Configuring security checks

You can enable various security checks for incoming TCP/UDP packets. The packet is dropped if the system detects the specified condition. Use the appropriate syntax for your FortiSwitch model:

- [Syntax \(for model FS112D-POE\) on page 47](#)
- [Syntax \(for all other FortiSwitch models\) on page 48](#)

Syntax (for model FS112D-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}
```

Variable	Description	Default
tcp-syn-data	TCP SYN packet contains additional data (possible DoS attack).	disable
tcp-udp-port-zero	TCP or UDP packet has source or destination port set to zero.	disable
tcp_flag_zero	TCP packet with all flags set to zero.	disable

Variable	Description	Default
tcp_flag_FUP	TCP packet with FIN, URG and PSH flag set.	disable
tcp_flag_SF	TCP packet with SYN and FIN flag set.	disable
tcp_flag_SR	TCP packet with SYN and RST flag set.	disable
tcp_frag_ipv4_icmp	Fragmented ICMPv4 packet.	disable
tcp_arp_mac_mismatch	ARP packet with MAC source address mismatch between the layer-2 header and the ARP packet payload.	disable

Syntax (for all other 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}

```

Variable	Description	Default
sip-eq-dip	TCP packet with source IP equal to destination IP.	disable
tcp_flag	DoS attack checking for TCP flags.	disable
tcp-port-eq	TCP packet with source and destination TCP port equal.	disable
tcp-flag-FUP	TCP packet with FIN, URG, and PSH flags set, and sequence number is zero.	disable
tcp-flag-SF	TCP packet with SYN and FIN flag set.	disable
v4-first-frag	DoS attack checking for IPv4 first fragment.	disable
udp-port-eq	IP packet with source and destination UDP port equal.	disable
tcp-hdr-partial	TCP packet with partial header.	disable
macsa-eq-macda	Packet with source MAC equal to destination MAC.	disable

Logging

FortiSwitchOS provides a robust logging environment that enables you to monitor, store, and report traffic information and FortiSwitch events, including attempted log ins and hardware status. Depending on your requirements, you can log to a number of different hosts.

To configure event logging using the GUI:

1. Go to *Log > Config*.

The screenshot shows the 'Log Configuration' page in the FortiSwitchOS GUI. The 'Event Type' section is active, with the 'Enable' checkbox checked. Under 'Categories', the following options are checked: Link, POE, Router, Spanning Tree, Switch, Switch Controller, System, and User. The 'Syslog' section below has the 'Enable' checkbox unchecked. An 'Apply' button is located at the bottom right of the configuration area.

2. Under *Event Type*, select *Enable*.
3. Under *Event Type*, select the categories of events that you want logged.
4. Select *Apply*.

To configure event logging using the CLI:

```
config log eventfilter
  set event {enable | disable}
  set link {enable | disable}
  set poe {enable | disable}
  set router {enable | disable}
  set spanning_tree {enable | disable}
  set switch {enable | disable}
  set switch_controller {enable | disable}
  set system {enable | disable}
  set user {enable | disable}
end
```

To view the event logs in the GUI:

Go to *Log > Event Log > System*, *Log > Event Log > Router*, or *Log > Event Log > User*.

To view the event logs in the CLI:

```
show log eventfilter
```

Syslog server

Syslog is an industry standard for collecting log messages for off-site storage. You can send logs to a single syslog server. The syslog server can be configured in the GUI or CLI. Reliable syslog (RFC 6587) can be configured only in the CLI.

To configure a syslog server in the GUI:

1. Go to *Log > Config*.

The screenshot shows the 'Log Configuration' GUI. It is divided into three main sections: 'Event Type', 'Categories', and 'Syslog'.
 - In the 'Event Type' section, the 'Enable' checkbox is checked.
 - In the 'Categories' section, there are two columns of checkboxes, all of which are checked: Link, POE, Router, Spanning Tree, Switch, Switch Controller, System, and User.
 - In the 'Syslog' section, the 'Enable' checkbox is unchecked.
 - An 'Apply' button is located at the bottom right of the configuration area.

2. Under *Syslog*, select *Enable*.
3. Select the severity of events to log.
4. Enter the IP address or fully qualified domain name in the *Server* field.
5. Enter the port number that the syslog server will use. By default, port 514 is used.
6. Select *Apply*.

To configure a syslog server in the CLI:

```
config log syslogd setting
  set status enable
  set server <IP address or FQDN of the syslog server>
  set port <port number that the syslog server will use for logging traffic>
  set facility <facility used for remote syslog>
  set source-ip <source IP address of the syslog server>
end
```

For example, to set the source IP address of a syslog server to have an IP address of 192.168.4.5:

```
config log syslogd setting
  set status enable
  set source-ip 192.168.4.5
end
```

To configure a reliable syslog server in the CLI:

```
config log syslogd setting
  set status enable
  set server <IP address or FQDN of the syslog server>
  set mode reliable
  set port <port number that the syslog server will use for logging traffic>
  set enc-algorithm {high | high-medium | low}
  set certificate <certificate_used_to_communicate_with_syslog_server>
end
```

For example:

```
config log syslogd setting
  set status enable
  set source-ip 192.168.4.5
  set mode reliable
  set port 6514 // This is the default port used for reliable syslog.
  set enc-algorithm high-medium
  set certificate "155-sub-client"
end
```

Fault relay support

Fault relays are normally closed relays. When the FSR-112D-POE loses power, the relay contact is in a closed state, and the alarm circuit is triggered.

Using SSH and the Telnet client

Starting in FortiSwitchOS 6.2.0, you can use both IPv4 and IPv6 addresses with SSH and Telnet. If the IPv6 address is a link-local address, you must specify an output interface using %. For example:

```
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
execute telnet fe80::926c:acff:fe7b:e059%vlan20 // vlan20 is the output interface.
execute telnet 1002::21
execute telnet 12.345.6.78
```

Configuring SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network.

The FortiSwitch SNMP implementation is read-only. SNMP v1-compliant and v2c-compliant SNMP managers have read-only access to FortiSwitch system information through queries and can receive trap messages from the FortiSwitch unit.

To monitor FortiSwitch system information and receive FortiSwitch traps, you must first compile the Fortinet and FortiSwitch management information base (MIB) files. A MIB is a text file that describes a list of SNMP data objects that are used by the SNMP manager. These MIBs provide information that the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiSwitch SNMP agent.

FortiSwitch core MIB files are available for download by going to *System > Config > SNMP > Settings* and selecting the *FortiSwitch MIB File* download link.

This chapter covers the following topics:

- [SNMP access on page 52](#)
- [SNMP agent on page 52](#)
- [SNMP community on page 53](#)

SNMP access

Ensure that the management VLAN has SNMP added to the access-profiles.

Using the GUI:

1. Go to *System > Network > Interface > Physical*.
2. Select *Edit* for the *mgmt* interface.
3. Select *SNMP* in the access section.
4. Select *Update*.

Using the CLI:

```
config system interface
  edit <name>
    set allowaccess <access_types>
  end
end
```

NOTE: Re-enter the existing allowed access types and add `snmp` to the list.

SNMP agent

Create the SNMP agent.

Using the GUI:

1. Go to *System > Config > SNMP > Settings*.
2. Select *Agent Enabled*.
3. Enter a descriptive name for the agent.
4. Enter the location of the FortiSwitch unit.
5. Enter a contact or administrator for the SNMP agent or FortiSwitch unit.
6. Select *Apply*.

Using the CLI:

```
config system snmp sysinfo
  set status enable
  set contact-info <contact_information>
  set description <description_of_FortiSwitch>
  set location <FortiSwitch_location>
end
```

SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a FortiGate SNMP and a FortiSwitch SNMP community.

Add SNMP communities to your FortiSwitch unit so that SNMP managers can connect to view system information and receive SNMP traps.

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

Adding an SNMP v1/v2c community

Using the GUI:

1. Go to *System > Config > SNMP > Communities*.
2. Select *Add Community*.
3. Enter a community name and identifier.
4. Select *Add Host* and enter the identifier, IP address and netmask, and interface for each host.
5. Select *V1*, *V2C*, or both and enter the port number that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiSwitch unit.
6. Select *V1*, *V2C*, or both and enter the local and remote port numbers that the FortiSwitch unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community.
7. Select which events to report.
8. Select *Add*.

Using the CLI:

```
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}
```

Adding an SNMP v3 user**Using the GUI:**

1. Go to *System > Config > SNMP > Users*.
2. Select *Add User*.
3. Enter a user name.
4. Select a security level to specify the authentication and privacy settings.
5. Enter the port number that the SNMP managers in this community use to receive configuration information from the FortiSwitch unit.
6. Make certain that *Enable Queries* is enabled.
7. Select *Add*.

Using the CLI:

```
config system snmp user
  edit <index_number>
    set queries enable
    set query-port <port_number>
    set security-level [auth-priv | auth-no-priv | no-auth-no-priv]
  end
```

Global system and switch settings

This chapter covers the following topics:

- Configuration file settings on page 55
- SSL configuration on page 55
- Configuration file revisions on page 56
- IP conflict detection on page 57
- Port flap guard on page 58
- Link monitor on page 61
- Unicast hashing on page 62
- Cut-through switching mode on page 62
- Enabling packet forwarding on page 62
- ARP timeout value on page 63
- Power over Ethernet configuration on page 63
- Creating a schedule on page 64
- Overlapping subnets on page 66

Configuration file settings

You can set preferences for saving configuration files:

1. Go to *System > Config > Backup*.
2. Select one of the Configuration Save options:
 - *Automatically Save*—The system automatically saves the configuration after each change.
 - *Manually Save*—You must manually save configuration changes from the *Backup* link on the *System > Dashboard*.
 - *Manually Save and Revert Upon Timeout*—You must manually save configuration changes. The system reverts to the saved configuration after a timeout. You can set the timeout using the CLI:

```
config system global
set cfg-revert-timeout <integer>
```
3. If you select *Revision Backup on Logout*, the FortiSwitch unit creates a configuration file each time a user logs out.
4. If you select *Revision Backup on Upgrade*, the FortiSwitch unit creates a configuration file before starting a system upgrade.
5. Select *Update*.

SSL configuration

You can set strong cryptography and select which certificates are used by the FortiSwitch unit.

Using the GUI:

1. Go to *System > Config > SSL*.
2. Select *Strong Crypto* to use strong cryptography for HTTPS and SSH access.
3. Select one of the 802.1x certificate options:
 - *Entrust_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.
 - *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.
 - *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.
 - *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.
4. Select one of the 802.1x certificate authority (CA) options:
 - *Entrust_802.1x_CA*—Select this CA if you are using 802.1x authentication.
 - *Entrust_802.1x_G2_CA*—Select this CA if you want to use the Google Internet Authority G2.
 - *Entrust_802.1x_L1K_CA*—Select this CA if you want to use <http://ocsp.entrust.net>.
 - *Fortinet_CA*—Select this CA if you want to use the factory-installed certificate.
 - *Fortinet_CA2*—Select this CA if you want to use the factory-installed certificate.
5. Select one of the GUI HTTPS certificate options:
 - *Entrust_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.
 - *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.
 - *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.
 - *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.
6. Select *Update*.

Using the CLI:

```

config system global
  set strong-crypto {enable | disable}
  set 802.1x-certificate {Entrust_802.1x | Fortinet_Factory | Fortinet_Factory2 |
    Fortinet_Firmware}
  set 802.1x-ca-certificate {Entrust_802.1x_CA | Entrust_802.1x_G2_CA | Entrust_802.1x_
    L1K_CA | Fortinet_CA | Fortinet_CA2}
  set admin-server-cert {self-sign | Entrust_802.1x | Fortinet_Factory | Fortinet_
    Factory2 | Fortinet_Firmware}
end

```

Configuration file revisions

You can select a configuration file revision to revert to.

Using the GUI:

1. Go to *System > Config > Revisions*.
The system displays a new page with an entry for each configuration file revision.
2. When you select a revision, the following commands are available:
 - *Deselect All*—deselect all selected revisions.
 - *Delete*—deletes the selected revision file.
 - *Revert*—reverts the system configuration to the selected revision.
 - *Upload*—uploads the selected revision file to your local machine.
3. If you select two revision files, you can select *Diff* to display the differences between the two files.

Using the CLI:

Use the following command to display the list of configuration file revisions:

```
execute revision list config
```

The FortiSwitch unit assigns a numerical ID to each configuration file. To display a particular configuration file contents, use the following command and specify the ID of the configuration file:

```
execute revision show config id <ID number>
```

The following example displays the list of configuration file revisions:

```
# execute revision list config

ID TIME ADMIN FIRMWARE VERSION COMMENT
1 2015-08-31 11:11:00 admin V3.0.0-build117-REL0 Automatic backup (session expired)
2 1969-12-31 16:06:29 admin V3.0.0-build150-REL0 baseline
3 2015-08-31 15:19:31 admin V3.0.0-build150-REL0 baseline
4 2015-08-31 15:28:00 admin V3.0.0-build150-REL0 with admin timeout
```

The following example displays the configuration file contents for revision ID 62:

```
# execute revision show config id 62

#config-version=FS1D24-3.04-FW-build171-160201:opmode=0:vdom=0:user=admin
#conf_file_ver=1784779075679102577
#buildno=0171
#global_vdom=1
config system global
    set admin-concurrent enable
    ...
(output truncated)
```

IP conflict detection

IP conflicts can occur when two systems on the same network are using the same IP address. The FortiSwitch unit monitors the network for conflicts and raises a system log message and an SNMP trap when it detects a conflict.

The IP conflict detection feature provides two methods to detect a conflict. The first method relies on a remote device to send a broadcast ARP (Address Resolution Protocol) packet claiming ownership of a particular IP address. If the IP address in the source field of that ARP packet matches any of the system interfaces associated with the receiving FortiSwitch system, the system logs a message and raises an SNMP trap.

For the second method, the FortiSwitch unit actively broadcasts gratuitous ARP packets when any of the following events occurs:

- System boot-up
- Interface status changes from down to up
- IP address change

If a system is using the same IP address, the FortiSwitch unit receives a reply to the gratuitous ARP. If it receives a reply, the system logs a message.

Configuring IP conflict detection

IP conflict detection is enabled on a global basis. The default setting is enabled.

Using the GUI:

1. Go to *Network > Settings*.
2. Select *Enable IP Conflict Detection*.
3. Select *Apply*.

Using the CLI:

```
config system global
    set detect-ip-conflict <enable|disable>
```

Viewing IP conflict detection

If the system detects an IP conflict, the system generates the following log message:

```
IP Conflict: conflict detected on system interface mgmt for IP address 10.10.10.1
```

Port flap guard

A flapping port is a port that changes status rapidly from up to down. A flapping port can create instability in protocols such as STP. If a port is flapping, STP must continually recalculate the role for each port. Flap guard also prevents unwanted access to the physical ports.

The port flap guard detects how many times a port changes status during a specified number of seconds, and the system shuts down the port if necessary. You can manually reset the port and restore it to the active state.

Retaining the triggered state

When the flap guard is triggered, the status for the port is shown as “triggered” in the output of the `diagnose flapguard status` command. By default, rebooting the switch resets the state of the flap guard and removes

the “triggered” state. You can change the setting so that the triggered state remains after a switch is rebooting until the port is reset. See [Resetting a port on page 60](#).

Using the GUI:

1. Go to *Switch > Flap Guard*.

Flap Guard

Retain Triggered State Across Reboot

Update

2. Select *Retain Triggered State Across Reboot*.
3. Select *Update* to save the change.

Using the CLI:

```
config switch global
    set flapguard-retain-trigger enable
end
```

Configuring the port flap guard

The port flap guard is configured and enabled on each port. The default setting is disabled.

The flap rate counts how many times a port changes status during a specified number of seconds. The range is 1 to 30 with a default setting of 5.

The flap duration is the number of seconds during which the flap rate is counted. The range is 5 to 300 seconds with a default setting of 30 seconds.

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select a port.
3. Select *Edit*.
4. Under Flap Guard, select *Enable*.

Flap Guard

Enable

Flap Duration (Seconds)

30

(5-300)

Flap Rate

5

(1-30)

5. Enter values for *Flap Duration (Seconds)* and *Flap Rate*.
6. Select *Update* to save the changes.

Using the CLI:

```
config switch physical-port
  edit <port_name>
    set flapguard {enabled | disabled}
    set flap-rate <1-30>
    set flap-duration <5-300 seconds>
  end
```

For example:

```
config switch physical-port
  edit port10
    set flapguard enabled
    set flap-rate 15
    set flap-duration 100
  end
```

Resetting a port

After the flap guard detects that a port is changing status rapidly and the system shuts down the port, you can reset the port and restore it to service.

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select the port that was shut down.
3. Select *Reset*.

Using the CLI:

```
execute flapguard reset <port_name>
```

For example:

```
execute flapguard reset port15
```

Viewing the port flap guard configuration

Use the following command to check if the flap guard is enabled on a specific port:

```
show switch physical-port <port_name>
```

For example:

```
show switch physical-port port10
```

Use the following command to display the port flap guard information for all ports:

```
diagnose flapguard status
```

Link monitor

You can monitor the link to a server. The FortiSwitch unit sends periodic ping messages to test that the server is available.

Configuring the link monitor

Using the GUI:

1. Go to *Router > Config > Link Probes*.
2. Select *Add Probe* to create a new probe.
3. Enter an IP address for the *Gateway IP*.
4. Configure the other fields as required (see the table in this section for field descriptions).
5. Select *Add* to create the probe.

Using the CLI:

```
config system link-monitor
  edit "1"
    set srcintf <string>
    set protocol (arp | ping)
    set gateway-ip <IP address>
    set source-ip <IP address>
    set interval <integer>
    set timeout <integer>
    set failtime <integer>
    set recoverytime <integer>
    set update-cascade-interface (enable | disable)
    set update-static-route (enable | disable)
    set status (enable | disable)
  next
end
```

Variable	Description
srcintf	Interface where the monitor traffic is sent.
protocol	Protocols used to detect the server. Select ARP or ping.
gateway-ip	Gateway IP used to PING the server.
source-ip	Source IP used in packet to the server.
interval	Detection interval in seconds. The range is 1-3600.
timeout	Detect request timeout in seconds. The range is 1-255.

Variable	Description
failtime	Number of retry attempts before bringing the server down. The range is 1-10.
recoverytime	Number of retry attempts before bringing the server up. The range is 1-10.
update-cascade-interface	Enable or disable update cascade interface.
update-static-route	Enable or disable update static route.
status	Enable or disable link monitor administrative status.

Unicast hashing

You can configure the trunk hashing algorithm for unicast packets to use the source port:

```
config switch global
  set trunk-hash-unicast-src-port {enable | disable}
end
```

Cut-through switching mode

By default, all FortiSwitch models use the store-and-forward technique to forward packets. This technique waits until the entire packet is received, verifies the content, and then forwards the packet.

The FSW-1024D, FSW-1048D, and FSW-3032D models also have a cut-through switching mode to reduce latency. This technique forwards the packet as soon as the switch receives it.

NOTE: For the FSW-3032D model, the cut-through switching mode is not supported on split ports.

To change the switching mode for the main buffer for these three models, use the following commands:

```
config switch global
  set packet-buffer-mode {store-forward | cut-through}
end
```

NOTE: Changing the switching mode might stop traffic on all ports during the change.

Enabling packet forwarding

NOTE: These commands apply only to the 200 Series and 400 Series.

If you want to use layer-3 interfaces and IGMP snooping on certain FortiSwitch models, you must enable the forwarding of reserved multicast packets and IPv6 neighbor-discovery packets to the CPU. These features are enabled by default.

```
config switch global
  set reserved-mcast-to-cpu {enable | disable}
```

```
set neighbor-discovery-to-cpu {enable | disable}
end
```

ARP timeout value

By default, ARP entries in the cache are removed after 300 seconds. Use the following commands to change the default ARP timeout value:

```
config system global
    set arp-timeout <seconds>
end
```

For example, to set the ARP timeout to 1,000 seconds:

```
config system global
    set arp-timeout 1000
end
```

Power over Ethernet configuration

Power over Ethernet (PoE) describes any system that passes electric power along with data on twisted pair Ethernet cabling. Doing this allows a single cable to provide both data connection and electric power to devices (for example, wireless access points, IP cameras, and VoIP phones).



PoE is only available on models with the POE suffix in the model number (for example, FS-108E-POE).

Using the GUI:

1. Go to *Switch > POE*.

POE Settings

Power Mode	<input checked="" type="radio"/> Priority-Based	
	<input type="radio"/> First Come, First Served	
Pre-Standard Detection	<input checked="" type="checkbox"/>	
Power Budget (W)	<input type="text" value="400"/>	(1-740)
Guard Band (W)	<input type="text" value="19"/>	(1-20)
Alarm Threshold (%)	<input type="text" value="80"/>	(0-100)

Update

2. Set the PoE power mode to priority based or first-come,first-served.

When power to PoE ports is allocated by priority, lower numbered ports have higher priority so that port 1 has the highest priority. When more power is needed than is available, higher numbered ports are disabled first.

When power to PoE ports is allocated by first-come, first-served (FCFS), connected PoE devices receive power, but new devices do not receive power if there is not enough power.

If both priority power allocation and FCFS power allocation are selected, the physical port setting takes precedence over the global setting.

3. Enable or disable PoE pre-standard detection.



PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FSW-548D-FPOE, FSW-524D-FPOE, FSW-108D-POE, FSW-224D-POE, FSW-108E-POE, FSW-108E-FPOE, FSW-124E-POE, and FSW-124E-FPOE.

For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.

4. Set the maximum power budget in Watts.
5. Enter the power in Watts to reserve in case of a spike in PoE consumption.
6. Enter the threshold (a specified percentage of the total power budget) above which an alarm event is generated.

If your FortiSwitch unit has a PoE sensor, you can set an alarm for when the current power budget exceeds a specified percentage of the total power budget. When this threshold is exceeded, log messages and SNMP traps are generated. The default threshold is 80 percent.

7. Select *Update*.

Using the CLI:

```
config switch global
  set poe-alarm-threshold <0-100 percent>
  set poe-power-mode {first-come-first-served | priority}
  set poe-guard-band <1-20 Watts>
  set poe-pre-standard-detect {disable | enable}
  set poe-power-budget <1-740 Watts>
end
```

Creating a schedule

Use schedules to control when policies are enforced. For example, you can use a schedule to control when an access control list policy is enforced.

NOTE: If the status of an ACL policy is inactive, the schedule is ignored.

You can create a one-time schedule, a recurring schedule, or a group schedule:

- Use a one-time schedule when you want a policy enforced for a specified period.
- Use a recurring schedule when you want a policy enforced for specified hours and days every week.
- Use a group schedule to combine one-time schedules and recurring schedules.

To create a one-time schedule:

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

For example:

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

To create a recurring schedule:

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

For example:

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

To create a group schedule:

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

For example:

```
config system schedule group
  edit group1
    set member schedule1 schedule2
  end
```

Overlapping subnets

You can use the `set allow-subnet-inteface` 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.

NOTE: Different interfaces cannot have overlapping IP addresses or subnets. The same IP address can be used on different switches.

For example:

```
config system global
  set admintimeout 480
  set allow-subnet-overlap enable
  set auto-isl enable
end
config system interface
  edit "mgmt"
    set ip 172.16.86.112 255.255.255.0
    set allowaccess ping https http ssh snmp telnet
    set type physical
    set alias "test"
    set snmp-index 27
  next
  edit "internal"
    set ip 10.0.1.112 255.255.255.0
    set allowaccess ping
    set type physical
    set alias "testing-2"
    set snmp-index 26
  next
end
```

Physical port settings

The following sections describe the configuration settings that are associated with FortiSwitch physical ports:

- [Configuring general port settings on page 67](#)
- [Configuring flow control and priority-based flow control on page 69](#)
- [Auto-module speed detection on page 70](#)
- [Setting port speed \(autonegotiation\) on page 70](#)
- [Configuring power over Ethernet on a port on page 71](#)
- [Energy-efficient Ethernet on page 73](#)
- [Diagnostic monitoring interface module status on page 73](#)
- [Configuring split ports on page 75](#)
- [Configuring QSFP low-power mode on page 77](#)

Configuring general port settings

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select the port to update and then select *Edit*.
3. Enter an optional description of the port in the *Description* field.
4. Select *Up* or *Down* for the *Administrative Status*.
5. Select *Update* to save your changes.

Using the CLI:

```
config switch physical-port
  edit <port_name>
    set status {up | down}
    set description <string>
    set max-frame-size <bytes_int>
  end
```

General port settings include:

- `status`—Administrative status of the port
- `description`—Text description for the port
- `max-frame-size`—Maximum frame size in bytes (between 68 and 9216)

NOTE: For the eight models in the 1xxE series, the `max-frame-size` command is under the `config switch global` command.

Viewing port statistics

Using the GUI:

Go to *Switch > Monitor > Port Stats*.

Port Stats

Select All
 Deselect All

Search:

Name	Received Packets	Received Bytes	Transmitted Packets	Transmitted Bytes
port1	0	0	0	0
port2	0	0	0	0
port3	0	0	0	0
port4	0	0	0	0
port5	0	0	0	0
port6	0	0	0	0
port7	0	0	0	0
port8	0	0	0	0
port9	0	0	0	0
port10	0	0	0	0
port11	0	0	0	0
port12	0	0	0	0
port13	0	0	0	0
port14	0	0	0	0
port15	0	0	0	0
port16	0	0	0	0
port17	0	0	0	0
port18	0	0	0	0
port19	0	0	0	0
port20	0	0	0	0
port21	0	0	0	0
port22	0	0	0	0
port23	0	0	0	0
port24	0	0	0	0
port25	0	0	0	0
port26	0	0	0	0
port27	0	0	0	0
port28	0	0	0	0
port29	0	0	0	0
port30	0	0	0	0
port31	0	0	0	0
port32	0	0	0	0
port33	0	0	0	0
port34	0	0	0	0
port35	0	0	0	0
port36	0	0	0	0
port37	0	0	0	0
port38	0	0	0	0
port39	0	0	0	0
port40	0	0	0	0
port41	0	0	0	0
port42	0	0	0	0
port43	0	0	0	0
port44	0	0	0	0
port45	0	0	0	0
port46	0	0	0	0
port47	0	0	0	0
port48	0	0	0	0
port49	0	0	0	0
port50	0	0	0	0
port51	0	0	0	0
port52	0	0	0	0
port53	0	0	0	0
port54	0	0	0	0
internal	0	0	13	10,416

Showing 1 to 55 of 55 entries

To clear the statistics on all ports, select *Select All* and then select *Reset Stats*.

To clear the statistics on some of the ports, select the ports and then select *Reset Stats*.

Using the CLI:

```
diagnose switch physical-ports port-stats list [<list_of_ports>]
```

For example:

```
diagnose switch physical-ports port-stats list 1,3,4-6
```

To clear all hardware counters (except for QoS, SNMP, and web GUI counters) on the specified ports:

```
diagnose switch physical-ports set-counter-zero [<list_of_ports>]
```

To restore hardware counters (except for QoS, SNMP, and web GUI counters) on the specified ports:

```
diagnose switch physical-ports set-counter-revert [<list_of_ports>]
```

Configuring flow control and priority-based flow control

Flow control allows you to configure a port to send or receive a “pause frame” (that is, a special packet that signals a source to stop sending flows for a specific time interval because the buffer is full). By default, flow control is disabled on all ports.

```
config switch physical-port
  edit <port_name>
    set flow-control {both | rx | tx | disable}
  end
```

Parameters enable flow control to do the following:

- `rx`—receive pause control frames
- `tx`—transmit pause control frames
- `both`—transmit and receive pause control frames

Priority-based flow control allows you to avoid frame loss by stopping incoming traffic when a queue is congested.

After you enable priority-based flow control, you then configure whether a port sends or receives a priority-based control frame:

```
config switch physical-port
  edit <port_name>
    set priority-based-flow-control enable
    set flow-control {both | rx | tx | disable}
  end
```

When priority-based flow control is disabled, 802.3 flow control can be used.

NOTE: Priority-based flow control does not support half-duplex speed. When FortiSwitch ports are set to autonegotiate the port speed (the default), priority-based flow control is available if the FortiSwitch model supports it. Lossless buffer management and traffic class mapping are not supported.

Auto-module speed detection

When you enable auto-module speed detection, the system reads information from the module and sets the port speed to the maximum speed that is advertised by the module. If the system encounters a problem when reading from the module, it sets the default speed (default value is platform specific).

When auto-module sets the speed, the system creates a log entry noting this speed.

NOTE: Auto-speed detection is supported on 1/10G ports, but not on higher speed ports (such as 40G).

Setting port speed (autonegotiation)

By default, all of the FortiSwitch user ports are set to autonegotiate the port speed. You can also manually set the port speed. The port speeds available differ, depending on the port and switch.

Using the GUI:

1. Go to *Switch > Port > Physical* and select the port.
2. Select *Edit*.
3. Select *Auto-Negotiation* or the appropriate port speed.
4. Select *Update*.

Using the CLI:

```
config switch physical-port
  edit <port>
    set speed {1000auto | 100full | 100half | 10full | 10half | auto | 10000cr |
              10000full | 10000sr | 1000full | auto-module}
  end
```

Viewing auto-module configuration

Display the status of auto-module using following command:

```
config switch physical-port
  edit port47
    show
  end
config switch physical-port
  edit "port47"
    set max-frame-size 16360
    set speed 10000full
  get
  name : port47
  description : (null)
  flow-control : both
  link-status : down
  lldp-transmit : disable
  max-frame-size : 16360
  port-index : 47
  speed : 10000full
```

```
status : up
end
```

Link-layer discovery protocol

The Fortinet data center switches support LLDP (transmission and reception). The link layer discovery protocol (LLDP) is a vendor-neutral layer-2 protocol that enables devices on a layer-2 segment to discover information about each other.

For details, refer to [LLDP-MED on page 113](#).

Configuring power over Ethernet on a port

You can enable PoE, configure dynamic guard band, and set the priority power allocation for a specific port.

The dynamic guard band is set automatically to the expected power of a port before turning on the port. So, when a PoE device is plugged in, the dynamic guard band is set to the maximum power of the device type based on the AF or AT mode. The AF mode DGB is 15.4 W, and the AT mode DGB is 36 W. When the FortiSwitch unit is fully loaded, the dynamic guard band prevents a new PoE device from turning on.

When power to PoE ports is allocated by priority, lower numbered ports have higher priority so that port 1 has the highest priority. When more power is needed than is available, higher numbered ports are disabled first.

When power to PoE ports is allocated by first-come, first-served (FCFS), connected PoE devices receive power, but new devices do not receive power if there is not enough power.

If both priority power allocation and FCFS power allocation are selected, the physical port setting takes precedence over the global setting.

Enabling or disabling PoE in the GUI

1. Go to *Switch > Port > Physical*.
2. Select a port and then select *Edit*.
3. For the POE Status, select *Enable* or *Disable*.
4. Select a power priority for the port. You can select *High Priority*, *Critical Priority*, or *Low 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.
5. Select *Update*.

Configuring PoE in the CLI

```
config switch physical-port
edit <port>
set poe-status {enable | disable}
set poe-port-mode {IEEE802_3AF | IEEE802_3AT}
set poe-port-priority {critical-priority | high-priority | low-priority}
set poe-pre-standard-detect {disable | enable}
end
```



PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FSW-548D-FPOE, FSW-524D-FPOE, FSW-108D-POE, FSW-224D-POE, FSW-108E-POE, FSW-108E-FPOE, FSW-124E-POE, and FSW-124E-FPOE.

For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.

Determining the PoE power capacity

Using the GUI:

Go to *Switch > Port > Physical*. The Power column displays the power capacity for each PoE port.

Using the CLI:

```
get switch poe inline
```

Resetting the PoE power

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select a port and then select *POE Reset*.
3. In the confirmation dialog box, select *Reset*.

Using the CLI:

```
execute poe-reset <port>
```

Displaying PoE information

Using the GUI:

Go to *Switch > Port > Physical* to see information about each PoE port. Hover over the traffic column to get specific values.

port44	Auto-Negotiation	↑	↑	0.00/0.00W	↓	—	—		Cable Diagnostic
port45	Auto-Negotiation	↑	↑	0.00/0.00W	↓	—	—		Cable Diagnostic
port46	Auto-Negotiation	↑	↑	0.00/0.00W	↓	—	—		Cable Diagnostic
port47	Auto-Negotiation	↑	↑	0.00/0.00W	↓	—	—		Cable Diagnostic
port48	Auto-Negotiation	↑	↑	0.00/0.00W	↑	1G	Full		Cable Diagnostic
port49	Max Speed Supported by Module	↑	N/A	N/A	↓	—	—		

Using the CLI:

```
diagnose switch poe status <port>
```

The following example displays the information for port 6:

```
diagnose switch poe status port6
```

```
Port(6) Power:4.20W, Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AT PD
Power Class: 4
Defined Max Power: 30.0W, Priority:3
Voltage: 54.00V
Current: 71mA
```

Energy-efficient Ethernet

When no data is being transferred through a port, Energy-efficient Ethernet (EEE) puts the data link in sleep mode to reduce the power consumption of the FortiSwitch unit. When data flows through the port, the port resumes using the normal amount of power. EEE works over standard twisted-pair copper cables and supports 10 Mbps, 100 Mbps, 1 Gps, and 10 Ge. EEE does not reduce bandwidth or throughput.

NOTE: EEE is not supported on SFP and QSFP modules.

To configure EEE in the CLI:

```
config switch physical-port
  edit <port_name>
    set energy-efficient-ethernet {enable | disable}
  end
```

For example, to use EEE on port 7:

```
config switch physical-port
  edit port7
    set energy-efficient-ethernet enable
  end
```

To check that EEE is enabled on port 7:

```
diagnose switch physical-ports eee-status port7
```

To check which ports have EEE enabled:

```
diagnose switch physical-ports eee-status
```

Diagnostic monitoring interface module status

With diagnostic monitoring interface (DMI), you can view the following information

- Module details (detail)
- Eeprom contents (eeprom)
- Module limits (limit)
- Module status (status)
- Summary information of all a port's modules (summary)

Using the GUI:

Go to *Switch > Monitor > Modules*.

Using the CLI:

Use the following commands to enable or disable DMI status for the port. If you set the status to `global`, the port setting will match the global setting:

```
config switch physical-port
edit <interface>
    set dmi-status {disable | enable | global}
end
```

Use the `get switch modules detail/status` command to display DMI information:

```
FS108E3W14000720 # get switch modules detail port10
```

```
-----
Port(port10)
identifier SFP/SFP+
connector Unk (0x00)
transceiver 1000-Base-T
encoding 8B/10B
Length Decode Common
length_smf_1km N/A
length_cable 100 meter
SFP Specific
length_smf_100m N/A
length_50um_om2 N/A
length_62um_om1 N/A
length_50um_om3 N/A
vendor FINISAR CORP.
vendor_oid 0x009065
vendor_pn FCLF-8521-3
vendor_rev A
vendor_sn PBR1X35
manuf_date 06/20/2007
```

The following is an example of the output for the `switch modules status` command:

```
FS108E3W14000720 # get switch modules status port9
```

```
-----
Port(port9)
alarm_flags 0x0040
warning_flags 0x0040
temperature 18.792969 C
voltage 3.315100 volts
laser_bias 0.750800 mAmps
tx_power -2.502637 dBm
rx_power -40.000000 dBm
options 0x000F ( TX_DISABLE TX_FAULT RX_LOSS TX_POWER_LEVEL1 )
options_status 0x000C ( RX_LOSS TX_POWER_LEVEL1 )
```

Configuring split ports

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

Notes

- Splitting ports is supported on the following FortiSwitch models:
 - 3032D (ports 5 to 28 are splittable)
 - 3032E (ports can be split into 4 x 25G when configured in 100G QSFP28 mode or can be split into 4 x 10G when configured in 40G QSFP mode)
 - 524D, 524D-FPOE (ports 29 and 30 are splittable)
 - 548D, 548D-FPOE (ports 53 and 54 are splittable)
 - 1048E (In the 4 x 100G configuration, ports 49, 50, 51, and 52 are splittable as 4 x 25G, 4 x 10G, 4 x 1G, or 2 x 50G. Only two of the available ports can be split.)
 - 1048E (In the 4 x 4 x 25G configuration, ports 49, 50, 51, and 52 are splittable as 4 x 4 x 25G or 2 x 50G. All four ports can be split, but ports 47 and 48 are disabled.)
 - 1048E (In the 6 x 40G configuration, ports 49, 50, 51, 52, 53, 54 are splittable as 4 x 10G or 4 x 1G.)

Use the `set port-configuration ?` command to check which ports are supported for each model.
- Currently, the maximum number of ports supported in software is 64 (including the management port). Therefore, only 10 QSFP ports can be split. This limitation applies to all of the models, but only the 3032D, the 3032E, and the 1048E models have enough ports to encounter this limit.
- Starting in FortiOS 6.2.0, splitting ports is supported in FortiLink mode (that is, the FortiSwitch unit managed by a FortiGate unit).

Configuring a split port

Use the following commands to configure a split port:

```
config switch phy-mode
  set port-configuration {default | disable-port54 | disable-port41-48 | 4x100G | 6x40G
    | 4x4x25G}
  set {<port-name>-phy-mode <single-port| 4x25G | 4x10G | 4x1G | 2x50G}
  ...
  (one entry for each port that supports split port)
end
```

The following settings are available:

- `disable-port54`—For 548D and 548D-FPOE, only port53 is splittable; port54 is unavailable.
- `disable-port41-48`—For 548D and 548D-FPOE, port41 to port48 are unavailable, but you can configure port53 and port54 in split-mode.
- `4x100G`—For 1048E, enable the maximum speed (100G) of ports 49 through 52. Ports 53 and 54 are disabled.
- `6x40G`—For 1048E, enable the maximum speed (40G) of ports 49 through 54.
- `4x4x25G`—For 1048E, enable the maximum speed (100G) of ports 49 through 52; each split port has a maximum speed of 25G. Ports 47 and 48 are disabled.
- `single-port`—Use the port at the full base speed without splitting it.

- 4x25G—For 100G QSFP only, split one port into four subports of 25 Gbps each.
- 4x10G—For 40G or 100G QSFP only, split one port into four subports of 10Gbps each.
- 4x1G—For 40G or 100G QSFP only, split one port into four subports of 1 Gbps each.
- 2x50G—For 100G QSFP only, split one port into two subports of 50 Gbps each.

In the following example, a FortiSwitch 3032D model 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
```

The system applies the configuration only after you enter the `end` command, displaying the following message:

```
This change will cause a ports to be added and removed, this will cause loss of
configuration on removed ports. The system will have to reboot to apply this
change.
Do you want to continue? (y/n)y
```

To configure one of the split ports, use the notation ".x" to specify the split port:

```
config switch physical-port
  edit "port1"
    set lldp-profile "default-auto-isl"
    set speed 40000full
```

```
next
edit "port2"
  set lldp-profile "default-auto-is1"
  set speed 40000full
next
edit "port3"
  set lldp-profile "default-auto-is1"
  set speed 40000full
next
edit "port4"
  set lldp-profile "default-auto-is1"
  set speed 40000full
next
edit "port5.1"
  set speed 10000full
next
edit "port5.2"
  set speed 10000full
next
edit "port5.3"
  set speed 10000full
next
edit "port5.4"
  set speed 10000full
next
end
```

Configuring QSFP low-power mode

On FortiSwitch models with QSFP (quad small form-factor pluggable) ports, you can enable or disable the low-power mode with the following CLI commands:

```
config switch physical-port
  edit <port_name>
    set qsfp-low-power-mode {enabled | disabled}
  end
```

For example:

```
config switch physical-port
  edit port12
    set qsfp-low-power-mode disabled
  end
```

Layer-2 interfaces

This chapter covers the following topics:

- [Switched interfaces on page 78](#)
- [Dynamic MAC address learning on page 79](#)
- [Persistent \(sticky\) MAC addresses on page 81](#)
- [Static MAC addresses on page 82](#)
- [Fortinet loop guard on page 82](#)

Switched interfaces

Default configuration will suffice for regular switch ports. By default, VLAN is set to 1, STP is enabled, and all other optional capabilities are disabled.

You can configure optional capabilities such as [Spanning Tree Protocol](#), [sFlow](#), [802.1x authentication](#), and [Private VLANs](#). These capabilities are covered in subsequent sections of this document.

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select one or more interfaces to update and select *Edit*.
If you selected more than one port, the port names are displayed in the name field, separated by commas.
3. Enter new values as required for the *Native VLAN* and *Allowed VLANs* fields.
4. Select *OK* to save your changes.

Using the CLI:

```
config switch interface
  edit <port>
    set native-vlan <vlan>
    set allowed-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
    set untagged-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
    set stp-state {enabled | disabled}
    set edge-port {enabled | disabled}
```

Viewing interface configuration

Using the GUI:

Go to *Switch > Interface > Physical*.

Using the CLI:

```
show switch interface <port>
```

Display port settings using following command:

```
config switch interface
  edit <port>
    get
```

Dynamic MAC address learning

You can enable or disable dynamic MAC address learning on a port. The existing dynamic MAC entries are deleted when you change this setting. If you disable MAC address learning, you can set the behavior for an incoming packet with an unknown MAC address (to drop or forward the packet).

You can limit the number of learned MAC addresses on an interface or VLAN. The limit ranges from 1 to 128. If the learning limit is set to zero (the default), no limit exists. When the limit is exceeded, the FortiSwitch unit adds a warning to the system log.

Configuring dynamic MAC address learning

Use the following CLI commands to configure dynamic MAC address learning:

```
config switch physical-port
  edit <port>
    set l2-learning (enable | disable)
    set l2-unknown (drop | forward)
  end
config switch interface
  edit <port>
    set learning-limit <0-128>
  end
config switch vlan
  edit <VLAN_ID>
    set learning {enable | disable}
    set learning-limit <0-128>
  end
```

NOTE: If you enable 802.1x MAC-based authorization on a port, you cannot change the `l2-learning` setting.

Changing when MAC addresses are deleted

By default, each learned MAC address is deleted after 300 seconds. The value ranges from 10 to 1000,000 seconds. Set the value to zero to not delete learned MAC addresses.

Use the following command to change this value:

```
config switch global
  set mac-aging-interval 200
end
```

Logging dynamic MAC address events

By default, dynamic MAC address events are not logged. When you enable logging for an interface, the following events are logged:

- When a dynamic MAC address is learned
- When a dynamic MAC address is moved
- When a dynamic MAC address is deleted

NOTE: Some dynamic MAC address events might take a long time to be logged. If too many events happen within a short period of time, some events might not be logged.

To enable the logging of dynamic MAC address events:

```
config switch interface
  edit <interface_name>
    set log-mac-event enable
  end
```

To view the log entries:

```
execute log display
```

Using the learning-limit violation log

If you want to see the first MAC address that exceeded a learning limit for an interface or VLAN, you can enable the learning-limit violation log for a FortiSwitch unit. Only one violation is recorded per interface or VLAN.

To enable or disable the learning-limit violation log, use the following commands. By default, the learning-limit violation log is disabled. 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.

NOTE: The `set log-mac-limit-violations` command is only displayed if your FortiSwitch model supports it.

```
config switch global
  set log-mac-limit-violations {enable | disable}
end
```

To view the content of the learning-limit violation log, use one of the following commands:

- `get switch mac-limit-violations all`—to see 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.
- `get switch mac-limit-violations interface <interface_name>`—to see the first MAC address that exceeded the learning limit on a specific interface
- `get switch mac-limit-violations vlan <VLAN_ID>`—to see the first MAC address that exceeded the learning limit on a specific VLAN. This command is only displayed if your FortiSwitch model supports it.

To reset the learning-limit violation log, use one of the following commands:

- execute `mac-limit-violation reset all`—to clear all learning limit violation logs
- execute `mac-limit-violation reset interface <interface_name>`—to clear the learning limit violation log for a specific interface
- execute `mac-limit-violation reset vlan <VLAN_ID>`—to clear the learning limit violation log for a specific VLAN

You can also specify how often the learning-limit violation log is reset, use the following commands:

```
config switch global
    set log-mac-limit-violations enable
    set mac-violation-timer <0-1500>
end
```

For example:

```
config switch global
    set log-mac-limit-violations enable
    set mac-violation-timer 60
end
```

Persistent (sticky) MAC addresses

You can make dynamically learned MAC addresses persistent when the status of a FortiSwitch port changes (goes down or up). By default, MAC addresses are not persistent.

NOTE: You cannot use persistent MAC addresses with 802.1x authentication.

Using the GUI:

1. Go to *Switch > MAC Entries*.
2. Select *Add MAC Entry* to create a new item.
3. Select an interface and enter a value for *MAC Address* and *VLAN*.
4. Select *Sticky*.
5. Select *Add* to create the MAC entry.

To delete the persistent MAC addresses instead of saving them in the FortiSwitch configuration file:

1. Go to *Switch > Monitor > Forwarding Table*.
2. In the *Unsaved sticky MACs on* field, select an interface or select *All*.
3. Select *Delete*.

Using the CLI:

Use the following command to configure the persistence of MAC addresses on an interface:

```
config switch interface
    edit <port>
        set sticky-mac <enable | disable>
    next
end
```

You can also save persistent MAC addresses to the FortiSwitch configuration file so that they are automatically loaded when the FortiSwitch unit is rebooted. By default, persistent entries are lost when a FortiSwitch unit is rebooted. Use the following command to save persistent MAC addresses for a specific interface or all interfaces:

```
execute sticky-mac save {all | interface <interface_name>}
```

Use the following command to delete the persistent MAC addresses instead of saving them in the FortiSwitch configuration file:

```
execute sticky-mac delete-unsaved {all | interface <interface_name>}
```

Static MAC addresses

You can configure one or more static MAC addresses on an interface.

Using the GUI:

1. Go to *Switch > MAC Entries*.
2. Select *Add MAC Entry* to create a new item.
3. Select an interface and enter a value for *MAC Address* and *VLAN*.
4. Select *Add* to create the MAC entry.

Using the CLI:

```
config switch static-mac
  edit <sequence_number>
    set description <optional_string>
    set interface <interface_name>
    set mac <static_MAC_address>
    set type {sticky | static}
    set vlan-id <VLAN_ID>
  end
```

For example:

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

Fortinet loop guard

A loop in a layer-2 network results in broadcast storms that have far-reaching and unwanted effects. Fortinet loop guard helps to prevent loops. When loop guard is enabled on a switch port, the port monitors its subtending network for any downstream loops.

The loop guard feature is designed to work in concert with STP rather than as a replacement for STP. Each port that has loop guard enabled will periodically broadcast loop guard data packets (LGDP) packets to its network. If a broadcast packet is subsequently received by the sending port, a loop exists downstream.

NOTE: If a port detects a loop, the system takes the port out of service to protect the overall network. The port returns to service after a configured timeout duration. If the timeout value is zero, you must manually reset the port.

By default, loop guard is disabled on all ports, and the timeout is set to zero.

Configuring loop guard

Using the GUI:

1. Go to *Switch > Interface > Physical* or *Switch > Interface > Trunk*.
2. Select one or more interfaces to update and then select *Edit*.
If you selected more than one port, the port names are displayed in the name field, separated by commas.
3. Select *Enable Loop Guard*.
4. Select *OK* to save your changes.

Using the CLI:

```
config switch interface
edit port <number>
set loop-guard <enabled|disabled>
set loop-guard-timeout <integer>
```

When loop guard takes a port out of service, the system creates the following log messages:

```
Loop Guard: loop detected on <port_name>. Shutting down <port_name>
```

Use the following command to reset a port that detected a loop:

```
execute loop-guard reset <port>
```

Viewing the loop guard configuration

Using the GUI:

Go to *Switch > Interface > Physical* and check the *Loop Guard* column.

Using the CLI:

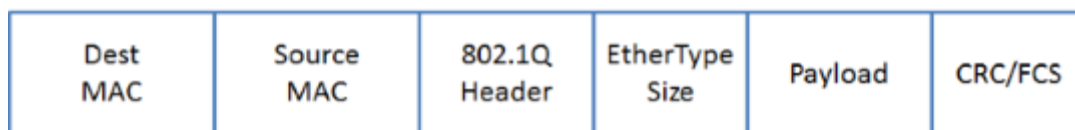
```
diagnose loop-guard instance status
```

VLANs and VLAN tagging

FortiSwitch ports process tagged and untagged Ethernet frames. Untagged frames do not carry any VLAN information.



Tagged frames include an additional header (the 802.1Q header) after the Source MAC address. This header includes a VLAN ID. This allows the VLAN value to be transmitted between switches.



The FortiSwitch unit provides port parameters to configure and manage VLAN tagging.

This chapter covers the following topics:

- [Native VLAN on page 84](#)
- [Allowed VLAN list on page 84](#)
- [Untagged VLAN list on page 85](#)
- [Packet processing on page 85](#)
- [Configuring VLANs on page 86](#)
- [Example 1 on page 86](#)
- [Example 2 on page 87](#)
- [VLAN stacking \(QinQ\) on page 88](#)

Native VLAN

You can configure a native VLAN for each port. The native VLAN is like a default VLAN for untagged incoming packets. Outgoing packets for the native VLAN are sent as untagged frames.

The native VLAN is assigned to any untagged packet arriving at an ingress port.

At an egress port, if the packet tag matches the native VLAN, the packet is sent out without the VLAN header.

Allowed VLAN list

The allowed VLAN list for each port specifies the VLAN tag values for which the port can transmit or receive packets.

For a tagged packet arriving at an ingress port, the tag value must match a VLAN on the allowed VLAN list or the native VLAN.

At an egress port, the packet tag must match the native VLAN or a VLAN on the allowed VLAN list.

Untagged VLAN list

The untagged VLAN list on a port specifies the VLAN tag values for which the port will transmit packets without the VLAN tag. Any VLAN in the untagged VLAN list must also be a member of the allowed VLAN list.

The untagged VLAN list applies only to egress traffic on a port.

Packet processing

Ingress processing ensures that the port accepts only packets with allowed VLAN values (untagged packets are assigned the native VLAN, which is implicitly allowed). At this point, all packets are now tagged with a valid VLAN.

The packet is sent to each egress port that can send the packet (because the packet tag value matches the native VLAN or an Allowed VLAN on the port).

Ingress port

Untagged packet

- packet is tagged with the native VLAN and allowed to proceed
- the Allowed VLAN list is ignored

Tagged packet

- tag VLAN value must match an Allowed VLAN or the native VLAN
- packet retains the VLAN tag and is allowed to proceed

To control what types of frames are accepted by the port, use the following commands:

```
config switch interface
  edit <interface>
    set discard-mode <all-tagged | all-untagged | none>
  end
```

Variable	Description
all-tagged	Tagged frames are discarded, and untagged frames can enter the switch.
all-untagged	Untagged frames are discarded, and tagged frames can enter the switch.
none	By default, all frames can enter the switch, and no frames are discarded.

Egress port

All packets that arrive at an egress port are tagged packets.

If the packet tag value is on the Allowed VLAN list, the packet is sent out with the existing tag.

If the packet tag value is the native VLAN or on the Untagged VLAN list, the tag is stripped, and then the packet is sent out.

Otherwise, the packet is dropped.

Configuring VLANs

Use the following steps to add VLANs to a physical port interface:

Using the GUI:

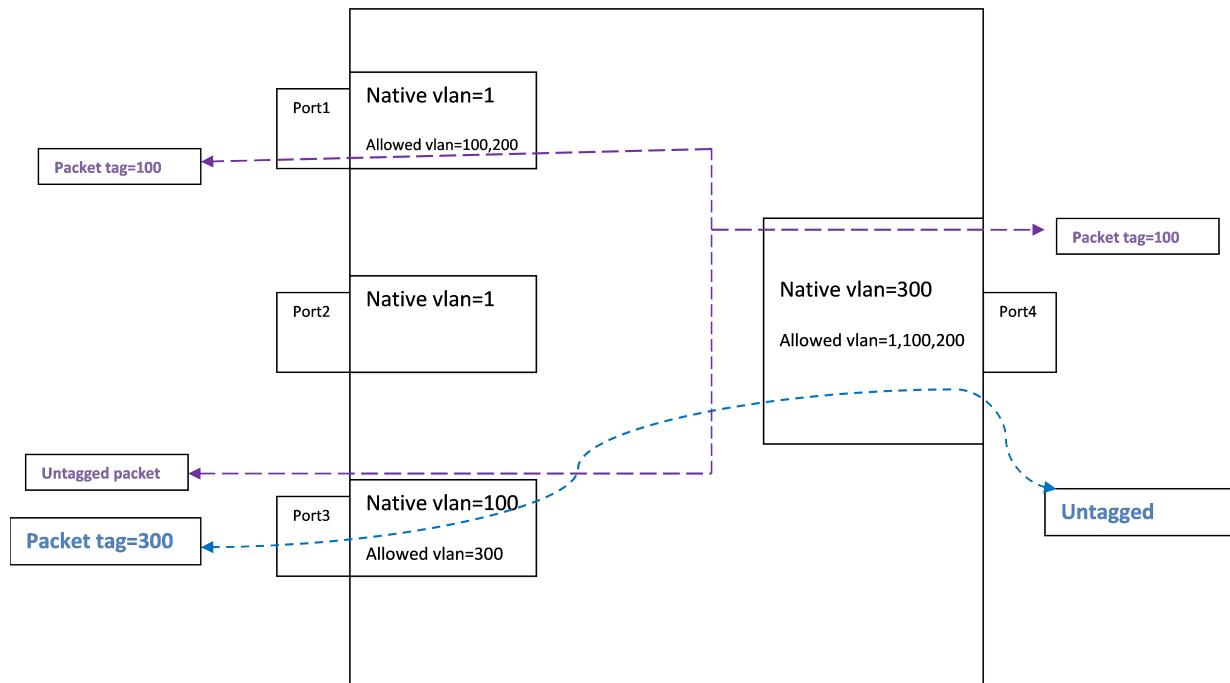
1. Go to *Switch > Interface > Physical*.
2. On the Physical Port Interfaces page, select a port and then select *Edit*.
3. Give the VLAN an appropriate name.
4. In the Native VLAN field, enter the identifier for the native VLAN of the port.
5. In the Allowed VLANs field, enter one or more identifiers for the allowed VLANs for the port. Separate multiple numbers with commas without any space. For example, 2, 4, 8-10.
6. In the Untagged VLANs field, enter one or more identifiers for the untagged VLANs for the port. Separate multiple numbers with commas without any space. For example, 2, 4, 8-10.
7. Select *OK*.

Using the CLI:

```
config switch interface
  edit <port>
    set native-vlan <vlan>
    set allowed-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
    set untagged-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
  end
```

Example 1

Example flows for tagged and untagged packets.



Purple flow

An untagged packet arriving at Port3 is assigned VLAN 100 (the native VLAN) and flows to all egress ports that will send VLAN 100 (Port1 and Port4).

A tagged packet (VLAN 100) arriving at Port4 is allowed (VLAN 100 is allowed). The packet is sent out from Port1 and Port3. On Port3, VLAN 100 is the native VLAN, so the packet is sent without a VLAN tag.

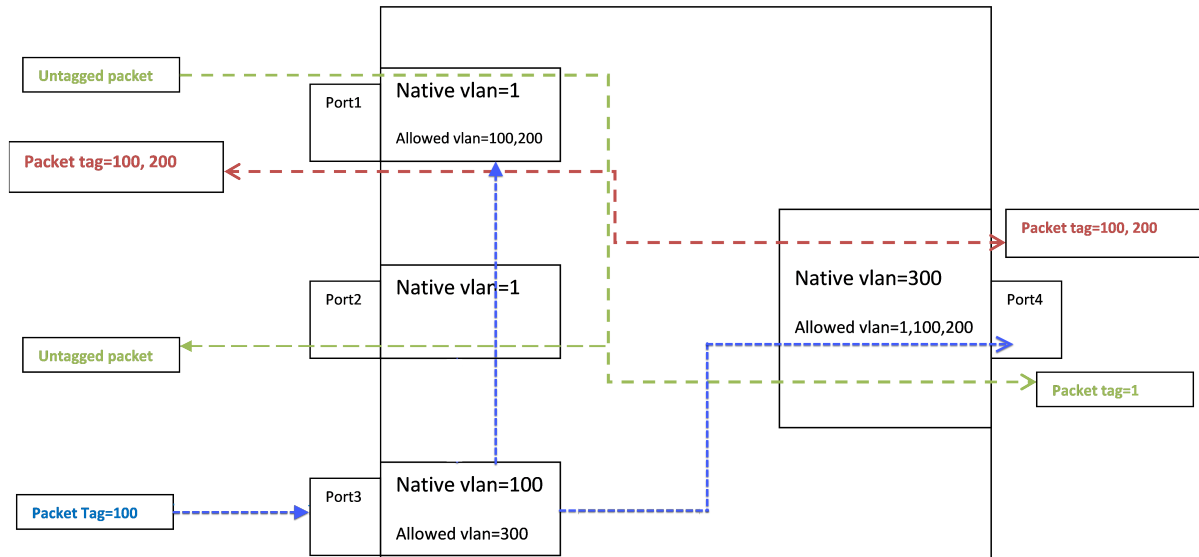
Blue flow

An untagged packet arriving at Port 4 is assigned VLAN 300 (the native VLAN). Then it flows out all ports that will send Vlan300 (Port 3).

A tagged packet (VLAN 300) arriving at Port3 is allowed. The packet is sent to egress from Port4. VLAN 300 is the native VLAN on Port4, so the packet is sent without a VLAN tag.

Example 2

Example of invalid tagged VLAN.



Green flow

Between Port1 and Port2, packets are assigned to VLAN 1 at ingress, and then the tag is removed at egress.

Blue flow

Incoming on Port 3, a tagged packet with VLAN value 100 is allowed, because 100 is the Port 3 native VLAN (the hardware VLAN table accepts a tagged or untagged match to a valid VLAN).

The packet will be sent on port1 and port4 (with packet tag 100).

VLAN stacking (QinQ)

VLAN stacking allows you to have multiple VLAN headers in an Ethernet frame. The value of the EtherType field specifies where the VLAN header is placed in the Ethernet frame.

Use the VLAN TPID profile to specify the value of 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.

NOTE: The following FortiSwitch models support VLAN stacking:

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, 3032E

NOTE: The following features are not supported with VLAN stacking:

- DHCP relay
- DHCP snooping
- IGMP snooping
- IP source guard

- PVLAN
- STP

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).

To configure VLAN stacking (asterisks indicate the default setting):

```

config switch interface
  edit <interface_name>
    set vlan-tpid <default | string>
  config qnq
    set status {enable | *disable}
    set vlan-mapping-miss-drop {enable | *disable}
    set add-inner <1-4095>
    set edge-type customer
    set stp-qnq-admin {*enable | disable}
    set priority {follow-c-tag | *follow-s-tag}
    set remove-inner {enable | *disable}
    config vlan-mapping
      edit <id>
        set description <string>
        set match-c-vlan <1-4094>
        set new-s-vlan <1-4094>
      next
    end
  end
next
end

```

Variable	Description	Default
<interface_name>	Enter the name of the interface.	No default
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. This setting is only for service-provider VLANs (S-VLANs). NOTE: 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
config qnq		
status {enable *disable}	Enable or disable VLAN stacking (QinQ) mode.	disable
vlan-mapping-miss-drop {enable *disable}	If the QinQ mode is enabled, 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

Variable	Description	Default
add-inner <1-4095>	If the QinQ mode is enabled, add the inner tag for untagged packets upon ingress.	No default
edge-type customer	If the QinQ mode is enabled, the edge type is set to customer.	customer
stp-qinq-admin {*enable disable}	Enable or disable VLAN stacking (QinQ) to manage the STP administration state.	enable
priority {follow-c-tag *follow-s-tag}	If the QinQ mode is enabled, select whether to follow the priority of the S-tag (service tag) or C-tag (customer tag).	follow-s-tag
remove-inner {enable *disable}	If the QinQ mode is enabled, enable or disable whether the inner tag is removed upon egress.	disable
<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
	Enter a new service (outer) VLAN.	
new-s-vlan <1-4094>	NOTE: 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

To configure VLAN mapping on an interface (asterisks indicate the default setting):

```

config switch interface
  edit <interface_name>
    set vlan-tpid <default | string>
    set vlan-mapping-miss-drop {enable | *disable}
    config vlan-mapping
      edit <id>
        set description <string>
        set direction ingress // ingress example
        set match-c-vlan <1-4094>
        set action {add | replace}
        set new-s-vlan <1-4094>
      next
      edit <id>
        set description <string>
        set direction egress // egress example
        set match-s-vlan <1-4094>
        set action {delete | replace}
        set new-s-vlan <1-4094>
      next
    end
  next
end

```

Variable	Description	Default
<interface_name>	Enter the name of the interface.	No default
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. This setting is only for service-provider VLANs (S-VLANs). NOTE: 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
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
config vlan-mapping		
<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: - <code>add</code> —When the packet is matched, add the service VLAN. You cannot set the <code>action</code> to <code>add</code> for the egress direction. - <code>delete</code> —When the packet is matched, delete the service VLAN. You cannot set the <code>action</code> to <code>delete</code> for the ingress direction. - <code>replace</code> —When the packet is matched, replace the customer VLAN or service VLAN. This option is only available after you set a value for <code>match-c-vlan</code> or <code>match-s-vlan</code> .	No default
new-s-vlan <1-4094>	Set the new service (outer) VLAN. This option is only available after you set the <code>action</code> to <code>add</code> or <code>replace</code> for the ingress direction or after you set the <code>action</code> to <code>replace</code> for the egress direction.	No default

To configure the VLAN TPID profile:

```
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

To check the VLAN stacking (QinQ) configuration:

```
diagnose switch qnq dtag-cfg
```

Spanning Tree Protocol

The FortiSwitch unit supports the following:

- Spanning Tree Protocol, a link-management protocol that ensures a loop-free layer-2 network topology
- Multiple Spanning Tree Protocol (MSTP), which is defined in the IEEE 802.1Q standard
- Per-VLAN Rapid Spanning Tree Protocol (also known as Rapid PVST or RPVST); RSTP is defined in the IEEE 802.1w standard

This chapter covers the following topics:

- [MSTP overview and terminology on page 93](#)
- [MSTP configuration on page 96](#)
- [Interactions outside of the MSTP region on page 101](#)
- [Viewing the MSTP configuration on page 102](#)
- [Support for interoperation with per-VLAN RSTP \(rapid PVST+ or RPVST+\) on page 102](#)

MSTP overview and terminology

MSTP supports multiple spanning tree instances, where each instance carries traffic for one or more VLANs (the mapping of VLANs to instances is configurable).

MSTP is backward-compatible with STP and Rapid Spanning Tree Protocol (RSTP). A layer-2 network can contain switches that are running MSTP, STP, or RSTP.

MSTP is built on RSTP, so it provides fast recovery from network faults and fast convergence times.

Regions

A region is a set of interconnected switches that have the same multiple spanning tree (MST) configuration (region name, MST revision number, and VLAN-to-instance mapping). A network can have any number of regions. Regions are independent of each other because the VLAN-to-instance mapping is different in each region.

The FortiSwitch unit supports 15 MST instances in a region. Multiple VLANs can be mapped to each MST instance. Each switch in the region must have the identical mapping of VLANs to instances.

The MST region acts like a single bridge to adjacent MST regions and to non-MST STPs.

IST

Instance 0 is a special instance, called the internal spanning-tree instance (IST). IST is a spanning tree that connects all of the MST switches in a region. All VLANs are assigned to the IST.

IST is the only instance that exchanges bridge protocol data units (BPDUs). The MSTP BPDU contains information for each MSTP instance (captured in an M-record). The M-records are added to the end of a regular RSTP BPDU. This allows MSTP region to inter-operate with an RSTP switch.

CST

The common spanning tree (CST) interconnects the MST regions and all instances of STP or RSTP that are running in the network.

Hop count and message age

MST does not use the BPDU message age within a region. The message-age and maximum-age fields in the BPDU are propagated unchanged within the region.

Within the region, a hop-count mechanism is used to age out the BPDU. The IST root sends out BPDUs with the hop count set to the maximum number of hops. The hop count is decremented each time the BPDU is forwarded. If the hop count reaches zero, the switch discards the BPDU and ages out the information on the receiving port.

STP port roles

STP assigns a port role to each switch port. The role is based on configuration, topology, relative position of the port in the topology, and other considerations. Based on the port role, the port either sends or receives STP BPDUs and forwards or blocks the data traffic. Here is a brief summary of each STP port role:

- **Designated**—One designated port is elected per link (segment). The designated port is the port closest to the root bridge. This port sends BPDUs on the link (segment) and forwards traffic towards the root bridge. In an STP converged network, each designated port is in the STP forwarding state.
- **Root**—The bridge can have only one root port. The root port is the port that leads to the root bridge. In an STP converged network, the root port is in the STP forwarding state.
- **Alternate**—Alternate ports lead to the root bridge but are not root ports. The alternate ports maintain the STP blocking state.
- **Backup**—This is a special case when two or more ports of the same switch are connected together (either directly or through shared media). In this case, one port is designated, and the remaining ports are backup (in the STP blocking state).

STP loop protection

The STP loop-protection feature provides additional protection against layer-2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state.

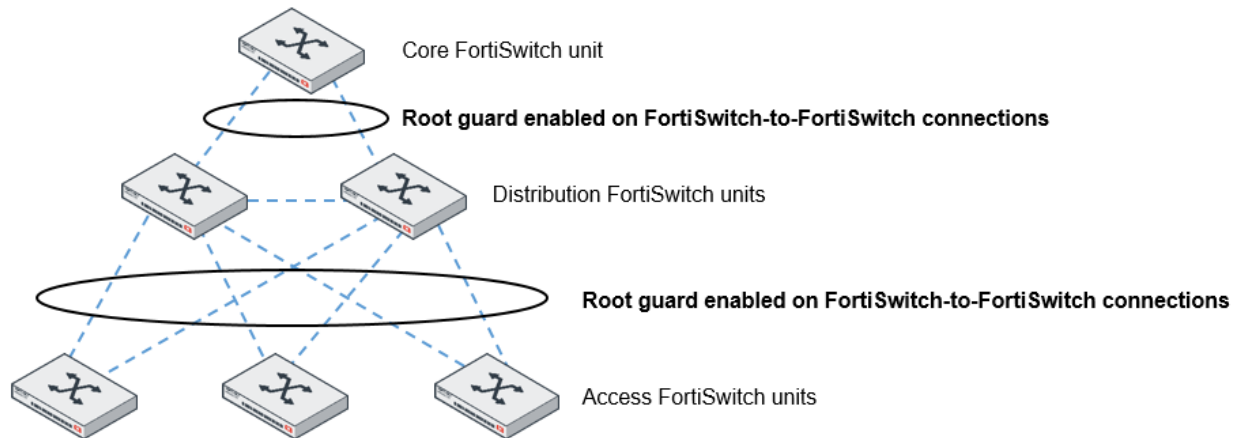
A port remains in blocking state only if it continues to receive BPDU messages. If it stops receiving BPDUs (for example, due to unidirectional link failure), the blocking port (alternate or backup port) becomes designated and transitions to a forwarding state. In a redundant topology, this situation may create a loop.

If the loop-protection feature is enabled on a port, that port is forced to remain in blocking state, even if the port stops receiving BPDU messages. It will not transition to forwarding state and does not forward any user traffic.

The loop-protection feature is enabled on a per-port basis. Fortinet recommends that you enable loop protection on all nondesignated ports (all root, alternate, and backup ports).

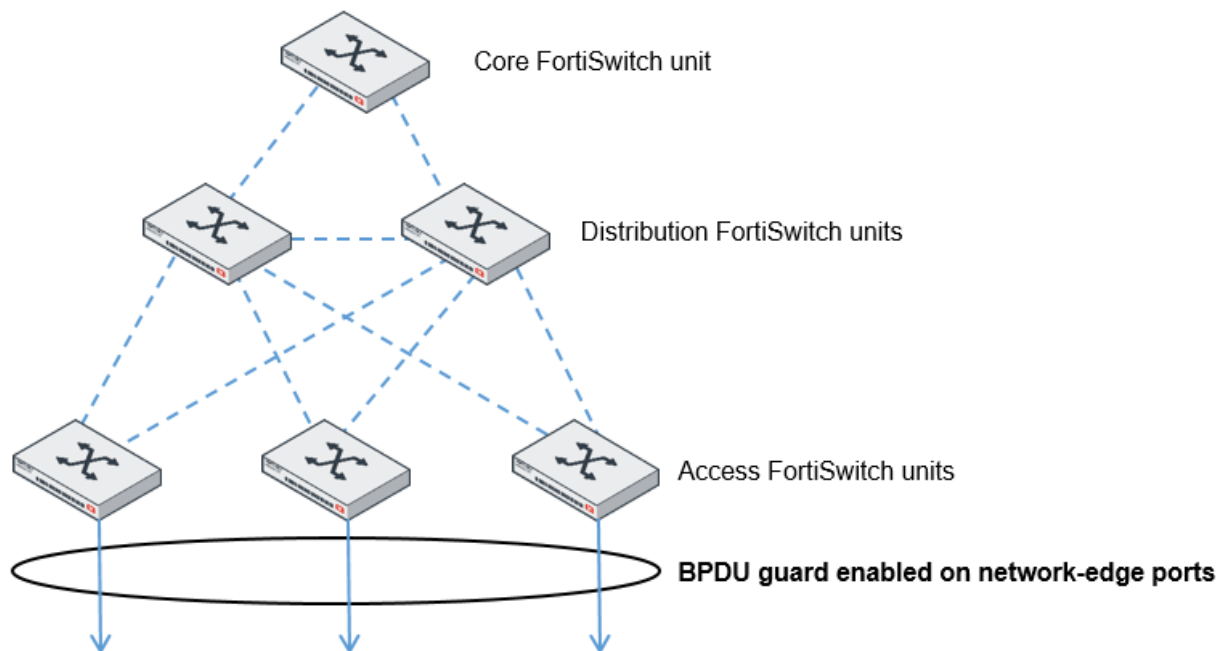
STP root guard

Root guard protects the interface on which it is enabled from becoming the path to root. When enabled on an interface, superior BPDUs received on that interface are ignored or dropped. Without using root guard, any switch that participates in STP maintains the ability to reroute the path to root. Rerouting might cause your network to transmit large amounts of traffic across suboptimal links or allow a malicious or misconfigured device to pose a security risk by passing core traffic through an insecure device for packet capture or inspection. By enabling root guard on multiple interfaces, you can create a perimeter around your existing paths to root to enforce the specified network topology.



STP BPDU guard

Similar to root guard, BPDU guard protects the designed network topology. When BPDU guard is enabled on STP edge ports, any BPDUs received cause the ports to go down for a specified number of minutes. The BPDUs are not forwarded, and the network edge is enforced.



MSTP configuration

MSTP configuration consists of the following steps:

1. Configure STP settings that are common to all MST instances.
2. Configure settings that are specific to each MST instance.
3. Configure loop-protection on all nondesignated ports.

Configuring STP settings

Some STP settings (region name and MST revision number) are common to all MST instances. Also, protocol timers are common to all instances because only the IST sends out BPDUs.

Using the GUI:

1. Go to *Switch > STP > Settings*.
2. Update the settings as described in the following table.
3. Select *Update* to save the settings.

Settings	Guidelines
Disabled	Disables MSTP for this switch.
Flood BPDU Packets	Select this checkbox if you want the STP packets arriving at any port to pass through the switch without being processed. If you do not select this checkbox, STP packets arriving at any port are blocked. This option is only available when MSTP is disabled.
Enabled	Enables MSTP for this switch.
Name	Region name. All switches in the MST region must have the identical name.
Revision	The MSTP revision number. All switches in the region must have the same revision number. The range of values is 0 to 65535. The default value is 0.
Hello Time (Seconds)	Hello time is how often (in seconds) that the switch sends out a BPDU. The range of values is 1 to 10. The default value is 2.
Forward Time (Seconds)	Forward time is how long (in seconds) a port will spend in the listening-and-learning state before transitioning to forwarding state. The range of values is 4 to 30. The default value is 15.

Settings	Guidelines
Max Age (Seconds)	The maximum age before the switch considers the received BPDU information on a port to be expired. Max-age is used when interworking with switches outside the region. The range of values is 6 to 40. The default value is 20.
Max Hops	Maximum hops is used inside the MST region. Hop count is decremented each time the BPDU is forwarded. If max-hops reaches zero, the switch discards the BPDU and ages out the information on the receiving port. The range of values is 1 to 40. The default value is 20.

Using the CLI:

```

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

```

Configuring an MST instance

The STP topology is unique for each MST instance in the region. You can configure a different bridge priority and port parameters for each instance.

Using the GUI:

1. Go to *Switch > STP > Instances*.
2. Select *Add Instance* to create a new MST instance or select an existing instance and then select *Edit*.
3. Update the instance parameters as described in the following table.
4. Select *Add* or *Update* to save the settings.

Settings	Guidelines
ID	Instance identifier. The range is 0-32 for 5xx models and higher. For all other models, the range is 0 - 15.
Priority	Priority is a component of bridge ID. The switch with the lowest bridge ID becomes the root switch for this MST instance. Allowed values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.

Settings	Guidelines
VLAN Range	The VLANs that map to this MST instance. You can specify individual VLAN numbers or a range of numbers. NOTE: Do not assign any VLAN to more than one MST instance. Each VLAN number is in the range 1-4094.
Port Configuration	
Name	Port that will participate in this MST instance.
Cost	The switch uses port cost to select designated ports. Port cost is added to the received BPDU root cost in any BPDU sent on this port. A lower value is preferred. The range of values is 1 to 200,000,000. The default value depends on the interface speed: - 10 Gigabit Ethernet: 2,000 - Gigabit Ethernet: 20,000 - Fast Ethernet: 200,000 - Ethernet: 2,000,000
Priority	The switch uses port priority to choose among ports of the same cost. The port with the lowest priority is put into forwarding state. The valid values are: 0, 32, 64, 96, 128, 160, 192, and 224. The default value is 128.

Using the CLI:

```

config switch stp instance
  edit <instance number>
    set priority <>
  config stp-port
    edit <port name>
      set cost <>
      set priority <>
    next
  set vlan-range <vlan range>
end

```

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
```

Configuring an STP edge port

You can use the edge-port setting when a device connected to a FortiSwitch port is not an STP bridge. When this setting is enabled, the FortiSwitch port immediately moves to a forwarding state rather than passing through listening and learning states.

By default, STP (and edge port) is enabled on all ports.

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. On the Physical Port Interfaces page, select a port and then select *Edit*.
3. Under Edge Port, select *Enable*.
4. Select *OK* to save the settings.

Using the CLI:

```
config switch interface
    edit <port_name>
        set edge-port <enabled | disabled>
    next
end
```

Configuring STP loop protection

By default, STP loop protection is disabled on all ports.

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. On the Physical Port Interfaces page, select a port and then select *Edit*.
3. Under Loop Guard, select *Enable*.
4. Select *OK* to save the settings.

Using the CLI:

```
config switch interface
    edit <port_name>
        set stp-loop-protection <enabled | disabled>
    next
end
```

Configuring STP root guard

Enable root guard on all ports that should not be root bridges. Do not enable root guard on the root port. You must have STP enabled to be able to use root guard.

Using the CLI:

```
config switch interface
  edit <port_name>
    set stp-root-guard <enable | disable>
  next
end
```

For example, to enable root guard on port 20:

```
config switch interface
  edit port20
    set stp-state enabled
    set stp-root-guard enable
  next
end
```

Configuring STP BPDU guard

There are three prerequisites for using BPDU guard:

- You must define the port as an edge port with the `set edge-port enabled` command.
- You must enable STP on the switch interface with the `set stp-state enabled` command.
- You must enable STP on the global level with the `set status enable` command.

You can set how long the port will go down for when a BPDU is received for a maximum of 120 minutes. The default port timeout is 5 minutes. If you set the timeout value to 0, the port will not go down when a BPDU is received, but you will have manually reset the port.

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. On the Physical Port Interfaces page, select a port and then select *Edit*.
3. Under Edge Port, select *Enable* and *BPDU Guard*.
4. In the Timeout (Minutes) field, enter how many minutes the port will go down for when a BPDU is received.
5. Select *OK* to save the settings.

Using the CLI:

```
config switch interface
  edit <port_name>
    set stp-bpdu-guard <enabled | disabled>
    set stp-bpdu-guard-timeout <0-120>
  next
end
```

For example, to enable BPDU guard on port 30 with a timeout value of 1 hour:

```
config switch stp settings
  set status enable
end
config switch interface
  edit port30
    set stp-state enabled
    set edge-port enabled
```

```

    set stp-bpdu-guard enabled
    set stp-bpdu-guard-timeout 60
  next
end

```

If you set the port timeout to 0, you will need to reset the port after it receives BPDUs and goes down. Use the following command to reset the port:

```
execute bpdu-guard reset <port_name>
```

To check if BPDU guard has been triggered and on which ports, use the following command:

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

Portname	State	Status	Timeout (m)	Count	Last-Event
port1	disabled	-	-	-	-
port2	disabled	-	-	-	-
port3	disabled	-	-	-	-
port4	disabled	-	-	-	-
port5	disabled	-	-	-	-
port6	disabled	-	-	-	-
port7	disabled	-	-	-	-
port8	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	-	-	-	-
port25	disabled	-	-	-	-
port26	disabled	-	-	-	-
port27	disabled	-	-	-	-
port28	disabled	-	-	-	-
port29	disabled	-	-	-	-
port30	enabled	-	60	0	-
__FoRtI1lLiNk0__	disabled	-	-	-	-

Interactions outside of the MSTP region

A boundary port on an MST switch is a port that receives an STP (version 0) BPDU, an RSTP (version 2) BPDU, or a BPDU from a different MST region.

If the port receives a version 0 BPDU, it will only send version 0 BPDUs on that port. Otherwise, it will send version 3 (MST) BPDUs because the RSTP switch will read this as an RSTP BPDU.

Viewing the MSTP configuration

To view the MSTP configuration details, use the following commands:

```
get switch stp instance
get switch stp settings
```

Use the following commands to display information about the MSTP instances in the network:

```
diagnose stp instance list
diagnose stp vlan list
diagnose stp mst-config list
```

Support for interoperation with per-VLAN RSTP (rapid PVST+ or RPVST+)

Starting in FortiSwitchOS 6.2.2, FortiSwitch units can now interoperate with a network that is running RPVST+. The existing network's configuration can be maintained while adding FortiSwitch units as an extended region.

When an MSTP domain is connected with an RPVST+ domain, FortiSwitch interoperation with the RPVST+ domain works in two ways:

- If the root bridge for the CIST is within an MSTP region, the boundary FortiSwitch unit of the MSTP region duplicates instance 0 information, creates one BPDU for every VLAN, and sends the BPDUs to the RPVST+ domain.

In this case, follow this rule: If the root bridge for the CIST is within an MSTP region, VLANs other than VLAN 1 defined in the RPVST+ domains must have their bridge priorities worse (numerically greater) than that of the CIST root bridge within MSTP region.

- If the root bridge for the CIST is within an RPVST+ domain, the boundary FortiSwitch unit processes only the VLAN 1 information received from the RPVST+ domain. The other BPDUs (VLANs 2 and above) sent from the connected RPVST+ domain are used only for consistency checks.

In this case, follow this rule: If the root bridge for the CIST is within the RPVST+ domain, the root bridge priority of VLANs other than VLAN 1 within that domain must be better (numerically less) than that of VLAN 1.

Configuring rapid PVST or RPVST+ interoperation support

Using the CLI:

Enable the RPVST+ interoperation support on the appropriate switch port or trunk.

```
config switch interface
  edit <interface_name>
    set allowed-vlans <one or more VLANs> // The VLANs must be configured for RSTP.
    set rpvst-port enabled
  next
```

```
end
```

For example, to enable RPVST+ interoperation support on port 9:

```
config switch interface
  edit "port9"
    set allowed-vlans 10,20
    set rpvst-port enabled
  next
end
```

For example, to enable RPVST+ interoperation support on trunk 1:

```
config switch interface
  edit "trunk1"
    set allowed-vlans 10,20
    set rpvst-port enabled
  next
end
```

Note: A maximum of 16 VLANs is supported; the maximum number of VLANs includes native VLANs. You must configure the same VLANs as those used in the RPVST+ domain.

Viewing the configuration

Use one of the following commands to check your configuration and to diagnose any problems.

- `diagnose stp instance list`

If either rule is violated, the RPVST port is flagged with “IC” in the command output, and the port is in the Discard state.

If the VLANs used by the RPVST+ domain are not all within the VLAN range configured on the RPVST port, an “MV” flag is displayed in the command output. **NOTE:** Only the ports in instance 0 show this flag.

- `diagnose stp rapid-pvst-port list`

This command shows 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 rapid-pvst-port clear`

This command clears all flags and timers on the RPVST+ port.

Link aggregation groups

This chapter provides information on how to configure a link aggregation group (LAG). For LAG control, The FortiSwitch unit supports the industry-standard Link Aggregation Control Protocol (LACP). The FortiSwitch unit supports LACP in active and passive modes. In active mode, you can optionally specify the minimum and maximum number of active members in a trunk group.

The FortiSwitch unit supports flap-guard protection for switch ports in a LAG.

This chapter covers the following topics:

- [Configuring the trunk and LAG ports on page 104](#)
- [Checking the trunk configuration on page 106](#)

Configuring the trunk and LAG ports



It is important to configure the trunk to prevent loops.

Using the GUI:

1. Go to *Switch > Port > Trunk* and select *Add Trunk*.
2. Give the trunk an appropriate name.
3. For the mode, select *Static*, *LACP Active*, *LACP Passive*, or *Fortinet Trunk*.
4. Add the required ports to the *Included* list.
5. Select *Create*.

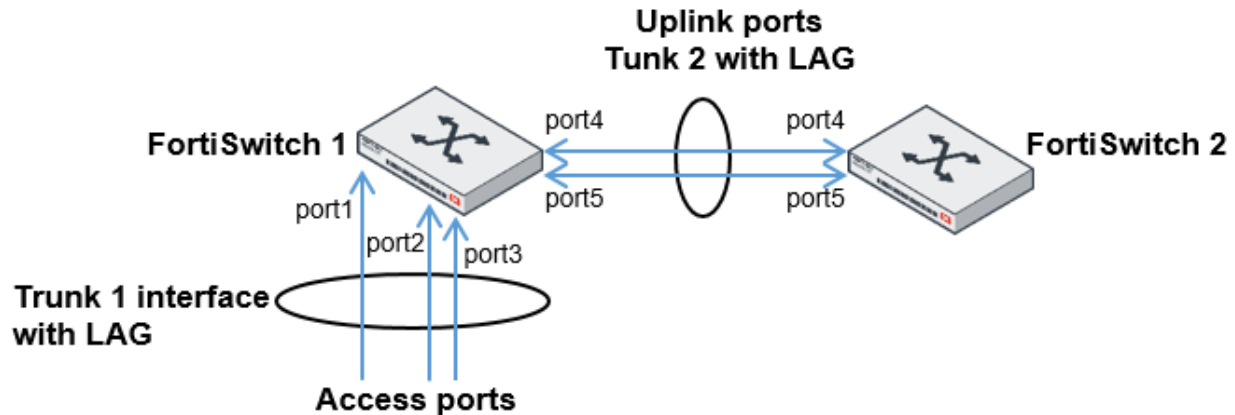
Using the CLI:

```
config switch trunk
  edit <trunk name>
    set description <description_string>
    set members <ports>
    set mode {lacp-active | lacp-passive | static}
    set member-withdrawal-behavior {block | forward}
    set lacp-speed {fast | slow}
    set bundle [enable|disable]
      set min_bundle <integer>
      set max_bundle <integer>
    set port-selection-criteria
      {src-ip | src-mac | dst-ip | dst-mac | src-dst-ip |src-dst-mac}
  end
end
```

Example configuration

The following is an example CLI configurations for trunk/LAG ports:

Trunk/LAG ports



1. Configure the trunk 1 interface and assign member ports as a LAG group:

```
config switch trunk
  edit trunk1
    set members "port1" "port2" "port3"
    set description test
    set mode lacp-passive
    set port-selection-criteria src-dst-ip
  end
```

2. Configure the switch ports to have native vlan assignments and allow those vlans on the port that will be the uplink port:

```
config switch interface
  edit port1
    set native-vlan 1
  next
  edit port2
    set native-vlan 2
  next
  edit port3
    set native-vlan 3
  next
  edit port4
    set native-vlan 4
    set allowed-vlans 1 2 3
  next
  edit port5
    set native-vlan 5
    set allowed-vlans 1 2 3
  end
end
```

3. Configure the trunk 2 interface and assign member ports as a LAG group:

```
config switch trunk
  edit trunk2
```

```
        set members "port4" "port5"
        set description test
        set mode lacp-passive
        set port-selection criteria src-dst-ip
    end
end
```

Checking the trunk configuration

Using the GUI:

Go to *Switch > Port > Trunk* or *Switch > Monitor > Trunks*.

Using the CLI:

```
diagnose switch trunk list
```

MCLAG

A link aggregation group (LAG) provides link-level redundancy. A multichassis LAG (MCLAG) provides node-level redundancy by grouping two FortiSwitch models together so that they appear as a single switch on the network. If either switch fails, the MCLAG continues to function without any interruption, increasing network resiliency and eliminating the delays associated with the Spanning Tree Protocol (STP).

This chapter covers the following topics:

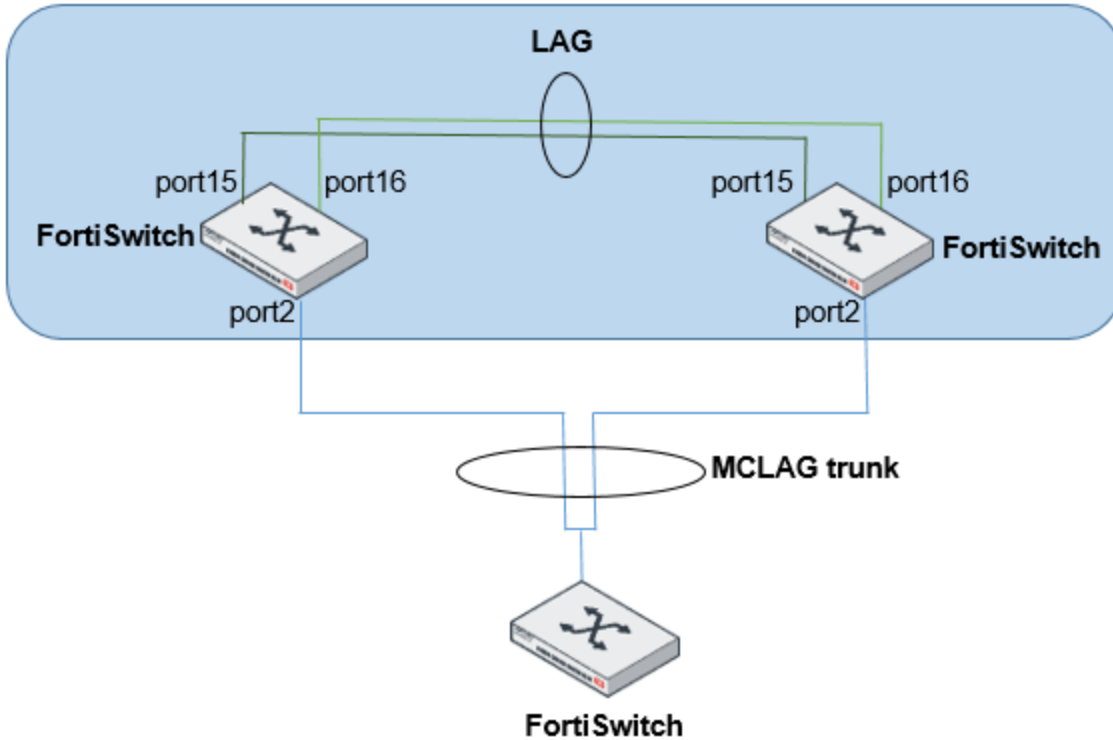
- [Notes on page 107](#)
- [Example configuration on page 108](#)
- [Viewing the configured trunk on page 109](#)
- [Configuring an MCLAG with IGMP snooping](#)

Notes

- When `min_bundle` or `max_bundle` is combined with MCLAG, the bundle limit properties are applied only to the local aggregate interface.
- Fortinet recommends that both peer switches be of the same hardware model and same software version. Mismatched configurations might work but are unsupported.
- There is a maximum of two FortiSwitch models per MCLAG.
- The routing feature is not available within a MCLAG.
- Starting in FortiSwitchOS 3.6.4, by default, the MCLAG can use the STP.
- To use static MAC addresses within a MCLAG, you need to configure MAC addresses on both switches that form the LAG.
- When you run an MCLAG, Fortinet recommends but does not require that peers use the same hardware and software versions. Some hosts might not be dual-home supported when MCLAG peers have different hardware; administrators need to size the layer-2 network to the MCLAG peer with the lowest capacity.

Example configuration

The following is an example CLI configurations for a MCLAG:



1. Create a LAG by configuring the ports for each FortiSwitch unit:

```
config switch trunk
  edit "MCLAG-ICL-trunk"
    set mclag-icl enable
    set members "port15" "port16"
    set mode lacp-active
  next
end
```

2. Set up the MCLAG:

```
config switch trunk
  edit "first-mclag"
    set mclag enable
    set members "port2"
  next
end
```

3. If you do not want the MCLAG to use the STP:

```
config switch global
  set mclag-stp-aware disabled
end
```

Viewing the configured trunk

Using the GUI:

Go to *Switch > Monitor > Trunks*.

Using the CLI:

```
diagnose switch mclag icl
diagnose switch mclag list
```

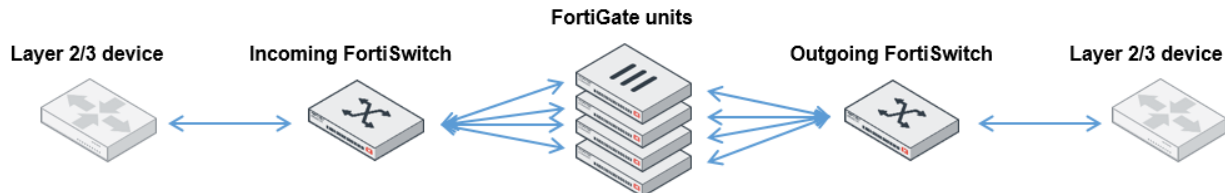
Configuring an MCLAG with IGMP snooping

For IGMP snooping to work correctly in an MCLAG, 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 MCLAG core FortiSwitch unit. For example:

```
config switch global
  set mac-aging-interval 600
  set mclag-igmpsnooping-aware enable
  config port-security
    set max-reauth-attempt 3
  end
end
config switch interface
  edit "D483Z15000094-0"
    set native-vlan 4094
    set allowed-vlans 1-4094
    set dhcp-snooping trusted
    set stp-state disabled
    set edge-port disabled
    set igmps-flood-reports enable
    set snmp-index 58
  next
end
```

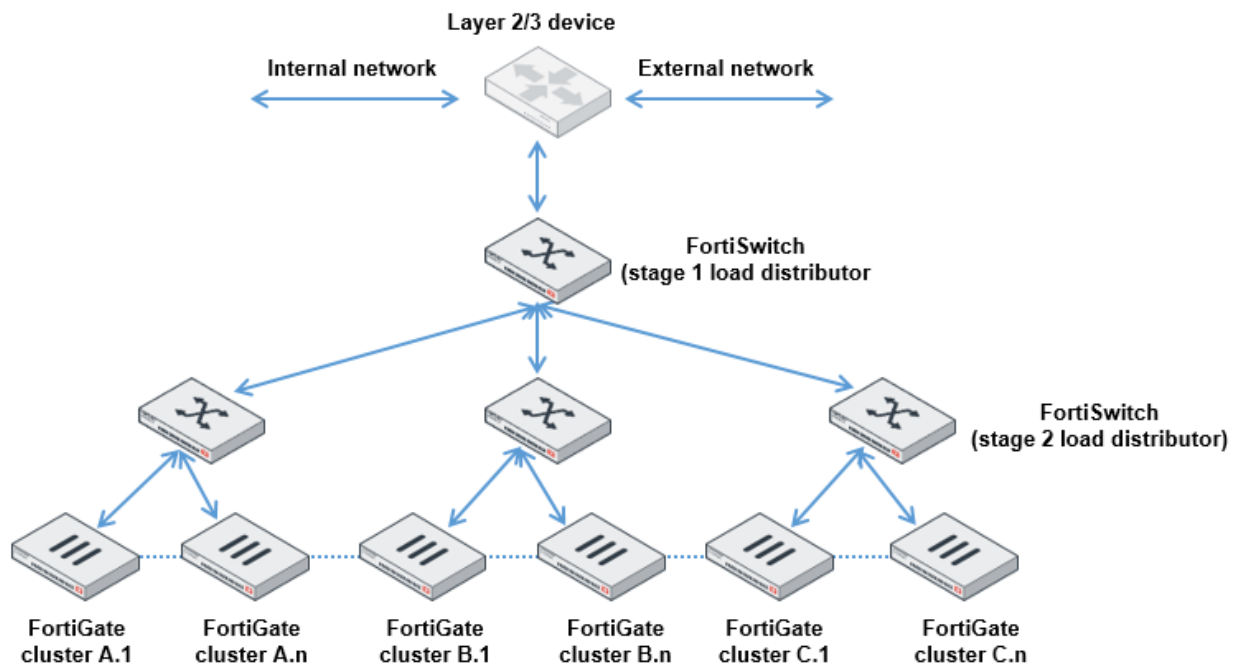
Multi-stage load balance

You can use a FortiSwitch unit to configure multi-stage load balancing on a set of FortiGate units. This capability allows you to scale security processing while maintaining a simple basic architecture. This configuration is commonly referred to a “firewall sandwich.”



Because the FortiGate unit provides session-aware analysis, the load distribution algorithm must be symmetric (traffic for a given session, in both directions, must all traverse the same FortiGate unit).

For larger scale deployment, the topology uses multiple layers of load distribution to allow for far larger numbers of FortiGate devices.



The hash at the first and second stages must be symmetric. The two stages must provide different hashing results.

This chapter covers the following topics:

- [Configuring the trunk ports on page 111](#)
- [Heartbeats on page 111](#)

Configuring the trunk ports

Use the following commands to configure the trunk members and set the port-selection criteria:

```
config switch trunk
  edit <trunk name>
    set description <description_string>
    set members <ports>
    set mode {fortinet-trunk | lacp-active | lacp-passive | static}
    set port-selection-criteria src-dst-ip-xor16
  end
end
```

Heartbeats

When in Fortinet-trunk mode, Heartbeat capability is enabled. Heartbeat messages monitor the status of FortiGate units. If one is unavailable, the FortiSwitch unit stops sending traffic to that FortiGate unit until the FortiGate unit becomes available.

If you enable `hb-verify`, each received heartbeat frame will be validated to match the signature (transmit-port plus switch serial number) and the following configured heartbeat parameters:

- `hb-in-vlan`
- `hb-src-ip`
- `hb-dst-ip`
- `hb-src-udp-port`
- `hb-dst-udp-port`

The destination MAC address of the heartbeat frame is set by default to 02:80:c2:00:00:02. You can change the value to any MAC address that is not a broadcast or multicast MAC address.

Configuring heartbeats

Configure the heartbeat fields using trunk configuration commands, as shown in this section. By default, all of the configurable values are set to zero, and `hb-verify` is disabled.

Set the mode to `forti-hb` and set the heartbeat loss limit to a value between 3 and 32.

The heartbeat will transmit at 1-second intervals on any link in the trunk that is up. This value is not configurable.

The heartbeat frame has configurable parameters for the layer-3 source and destination addresses and the layer-4 UDP ports. You must also specify the transmit and receive VLANs.

```
config switch trunk
  edit hb-trunk
    set mode fortinet-trunk
    set members <port> [<port>] ... [<port>]
    set hb-loss-limit <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
```

Use the following command to configure the destination MAC address:

```
config switch global
    set forti-trunk-dmac <mac address>
end
```

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
```

LLDP-MED

The Fortinet data center switches support the Link Layer Discovery Protocol (LLDP) for transmission and reception wherein the switch will multicast LLDP packets to advertise its identity and capabilities. A switch receives the equivalent information from adjacent layer-2 peers.

Fortinet data center switches support LLDP-MED (Media Endpoint Discovery), which is an enhancement of LLDP that provides the following facilities:

- Auto-discovery of LAN policies (such as VLAN, layer-2 priority, and differentiated services settings), to enable plug-and-play networking.
- Device location discovery to allow the creation of location databases and Enhanced 911 services for Voice over Internet Protocol (VoIP).
- Extended and automated power management for power over Ethernet (PoE) endpoints.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

The switch will multicast LLDP packets to advertise its identity and capabilities. The switch receives the equivalent information from adjacent layer-2 peers.

Starting in FortiSwitch 6.2.0, you can use the CLI to configure the location table used by LLDP-MED for enhanced 911 emergency calls.

This chapter covers the following topics:

- [Configuration notes on page 113](#)
- [LLDP global settings on page 114](#)
- [Configuring LLDP profiles on page 116](#)
- [Configuring an LLDP profile for the port on page 119](#)
- [Enabling LLDP on a port on page 120](#)
- [Checking the LLDP configuration on page 121](#)
- [Configuration deployment example on page 121](#)
- [Checking LLDP details on page 123](#)
- [LLDP OIDs on page 123](#)

Configuration notes

NOTE: When 802.1x and LLDP turn on at the same port, switching between LLDP profiles requires a manual reset of all authentication sessions.

Fortinet recommends LLDP-MED-capable phones.

The FortiSwitch unit functions as a Network Connectivity device (that is, NIC, switch, router, and gateway), and will only support sending TLVs intended for Network Connectivity devices.

LLDP supports up to 16 neighbors per physical port.

The FortiSwitch unit accepts and parses packets using the CDP (Cisco Discovery Protocol) and count CDP neighbors towards the neighbor limit on a physical port. If neighbors exist, the FortiSwitch unit transmits CDP packets in addition to LLDP.

With release 3.5.1, CDP is independently controllable through **cdp-status** on the physical port. The FortiSwitch unit no longer requires a neighbor to trigger it to transmit CDP; it will transmit provided **cdp-status** is configured as tx-only or tx-rx. The default configuration for CDP-status is disabled. It still uses values pulled from the lldp-profile to configure its contents.

LLDP must be globally enabled in `switch.lldp.settings` for CDP to be transmitted or received:

NOTE: If a port is added into a *virtual-wire* (connects two ends of a controlled system using a radio frequency [RF] medium), the FortiSwitch unit will disable the transmission and receipt of LLDP and CDP packets and remove all neighbors from the port. This virtual-wire state is noted in the `get switch lldp neighbor-summary` command output.

If the combination of configured TLVs exceeds the maximum frame size on a port, that frame cannot be sent.

LLDP global settings

Using the GUI:

1. Go to *Switch > LLDP MED > Settings*.
2. Select or clear *Enable LLDP Transmit/Receive*.
3. Select the management interface.
4. Enter a value in the *Transmit Hold* field.
5. Enter the number of seconds for the transmit interval.
6. Select or clear *Fast Start*. If you select *Fast Start*, enter the number of seconds.
7. Select *Update*.

Using the CLI:

```
config switch lldp settings
  set status {enable | disable}
  set tx-hold <int>
  set tx-interval <int>
  set fast-start-interval <int>
  set management-interface <layer-3 interface>
end
```

Variable	Description
status	Enable or disable
tx-hold	Number of tx-intervals before the local LLDP data expires (that is, the packet TTL (in seconds) is tx-hold times tx-interval). The range for tx-hold is 1 to 16, and the default value is 4.

Variable	Description
tx-interval	Frequency of LLDP PDU transmission ranging from 5 to 4095 seconds (default is 30).
fast-start-interval	How often the FortiSwitch unit transmits the first four LLDP packets when a link comes up. The range is 2 to 5 seconds, and the default is 2 seconds. Set this variable to zero to disable fast start.
management-interface	Primary management interface advertised in LLDP and CDP PDUs.

Setting the asset tag

To help identify the unit, LLDP uses the asset tag, which can be at most 32 characters. It will be added to the LLDP-MED inventory TLV (when that TLV is enabled):

```
config system global
    set asset-tag <string>
end
```

Configuring the location table

Because mobile phones have no fixed addresses associated with them, calls to 911 need the location information provided in emergency location identifier numbers (ELINs). You need to first configure the location table used by LLDP-MED for enhanced 911 emergency calls and then configure the LLDP profile to use the location table.

```
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
```

For example:

```
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
```

Configuring LLDP profiles

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.

Two static LLDP profiles, default and default-auto-isl, are created automatically. They can be modified but not deleted. The default-auto-isl profile always has auto-isl enabled and rejects any configurations that attempt to disable it.

LLDP-MED network policies

LLDP-MED network policies cannot be deleted or added. To use a policy, set the `med-tlvs` field to include `network-policy` and the desired network policy to `enabled`. The VLAN values on the policy are cross-checked against the VLAN native and untagged attributes for any interfaces that contain physical-ports using this profile. The cross-check determines if the policy Type Length Value (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 either a switch interface changes VLAN configuration or a physical port is added to, or removed from, a trunk.

The FortiSwitch unit supports the following LLDP-MED TLVs:

- Inventory Management TLVs
- Location Identification TLVs
- Network Policy TLV
- Power Management TLVs

Refer to the [Configuration deployment example on page 121](#).

Custom TLVs (organizationally specific TLVs)

Custom TLVs are configured in their own subtable, available in each profile. They allow you to emulate the TLVs defined in various specifications by using their OUI and subtype and ensuring that the data is formatted correctly. You could also define a purely arbitrary custom TLV for some other vendor or for their company.

The “name” value for each custom TLV is neither used by nor has an effect on LLDP; it simply differentiates between custom TLV entries:

```
config custom-tlvs
  edit <TLVname_str>
    set information-string <hex-bytes>
    set oui <hex-bytes>
    set subtype <integer>
  next
```

The OUI value for each TLV must be set to three bytes. If just one of those bytes is nonzero it is accepted; any value other than "000" is valid. The subtype is optional and ranges from 0 (default) to 255. The information string can be 0 to 507 bytes, in hexadecimal notation.

The FortiSwitch unit does not check for conflicts either between custom TLV values or with standardized TLVs. That is, other than ensuring that the OUI is nonzero, the FortiSwitch unit does not check the OUI, subtype (or data) values entered in the CLI for conflicts with other Custom TLVs or with the OUI and subtypes of TLVs defined by the 802.1, 802.3, LLDP-MED, or other standards. While this behavior could cause LLDP protocol issues, it also allows a large degree of flexibility were you to substitute a standard TLV that is not supported yet.

802.1 TLVs

The only 802.1 TLV that can be enabled or disabled is `port-vlan-id`. This TLV will send the native VLAN of the port. This value is updated when the native VLAN of the interface representing the physical port changes or if the physical port is added to, or removed from, a trunk.

By default, no 802.1 TLVs are enabled.

802.3 TLVs

The only 802.3 TLV that can be enabled or disabled is max-frame-size. This TLV will send the max-frame-size value of the port. If this variable is changed, the sent value will reflect the updated value.

By default, no 802.3 TLVs are enabled.

Auto-ISL

The auto-ISL configuration that was formerly in the `switch physical-port` command has been moved to the `switch lldp-profile` command. All behavior and default values are unchanged.

Assigning a VLAN to a port in the LLDP profile

You can configure the network policy of an LLDP profile to assign the specified VLAN to ports that use the LLDP profile. The VLAN is added as though it were configured in the `set allowed-vlans` setting in the `config switch interface` configuration.

This feature has the following requirements:

- The port cannot belong to a trunk or virtual wire.
- The port must have `lldp-status` set to `rx-only`, `tx-only`, or `tx-rx`.
- The port must have `private-vlan` set to `disabled`.
- LLDP must be enabled under the `config switch lldp settings` command.
- The `set med-tlvs network-policy` option must be set under the `config switch lldp profile` configuration.
- The `assign-vlan` option must be enabled in the `med-network-policy` configuration under the `config switch lldp profile` configuration.
- The VLAN assigned in the LLDP profile must be a valid VLAN.

Note:

- If the VLAN added to the interface by the LLDP profile is also listed under the `set untagged-vlans` configuration in the `config switch interface` command, the VLAN is added as untagged.
- If the VLAN added to the interface by the LLDP profile is also the native VLAN of the port, no changes occur.
- The LLDP service determines the contents of the network-policy TLV being sent based on the current state of the switch interface. If the LLDP VLAN assignment does not happen or the assigned VLAN is changed by another configuration (such as the `set untagged-vlans` configuration in `config switch interface`), the LLDP network policy TLVs being sent will reflect the actual state of the interface, not the configured value.

To specify a VLAN in the network policy of an LLDP profile:

```
config med-network-policy
  edit <policy_type_name>
    set status enable
    set assign-vlan enable
    set dscp <0-63>
    set priority <0-7>
    set vlan <0-4094>
  next
```

For example:

```
config med-network-policy
  edit default
    set status enable
    set assign-vlan enable
    set vlan 15
    set dscp 30
    set priority 3
  next
```

Configuring an LLDP profile for the port

Configure an LLDP profile for the port. By default, the port uses the default LLDP profile.

Using the GUI:

1. Go to *Switch > LLDP-MED > Profiles*.
2. Select *Add Profile*.
3. Enter a name for your LLDP profile.
4. If needed, select *Port VLAN ID*.
5. If needed, select *Maximum Frame Size*.
6. If needed, select *Enable* for Auto-ISL.
7. Enter the number of seconds for the Auto-ISL Hello Timer.
8. Enter the port group number for the Auto-ISL Port Group.
9. Enter the number of seconds for the Auto-ISL Receive Timeout.
10. If needed, select *Inventory Management*, *Network Policy*, or both.
11. Select *Add*.

Using the CLI:

```
config switch lldp profile
  edit <profile>
    set 802.1-tlvs port-vlan-id
    set 802.3-tlvs max-frame-size
    set auto-isl {active | inactive}
    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)
  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 <policy_type_name>
        set status {enable | disable}
        set assign-vlan {enable | disable}
        set dscp <0-63>
        set priority <0-7>
        set vlan <0-4094>
    next
end
```

Enabling LLDP on a port

To enable LLDP MED on a port, set the LLDP status to receive-only, transmit-only, or receive and transmit. The default value is TX/RX.

The CLI also supports power over Ethernet (PoE) negotiation in LLDP-MED for the following models: 548D-FPOE, 524D-FPOE, 108E-POE, 108E-FPOE, 124E-POE, 124E-FPOE, and 112D-POE.

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select a port and select *Edit*.
3. Select *TX/RX*, *RX Only*, *TX Only*, or *Disable* for the LLDP-MED status.
4. Select an LLDP profile.
5. Select *Update*.

Using the CLI:

```
config switch physical-port
    edit <port>
        set lldp-status (rx-only | tx-only | tx-rx | disable)
        set lldp-profile <profile name>
        set poe-lldp-detection {enable | disable}
    next
end
```

Checking the LLDP configuration

View the LLDP configuration settings using the GUI:

1. Go to *Switch > LLDP-MED > Settings*.
2. Make any changes that are needed.
3. Select *Update*.

View the LLDP configuration settings using the CLI:

```
get switch lldp settings
status : enable
tx-hold : 4
tx-interval : 30
fast-start-interval : 2
management-interface: internal
```

View the LLDP profiles using the GUI:

1. Go to *Switch > LLDP-MED > Profiles*.
2. Select a profile and then select *Edit*.
3. Make any changes that are needed.
4. Select *Update*.

View the LLDP profiles using the CLI:

```
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:
```

Use the following commands to display the LLDP information about LLDP status or the layer-2 peers for this FortiSwitch unit:

```
get switch lldp (auto-isl-status | neighbors-detail | neighbors-summary | profile |
settings | stats)
```

Configuration deployment example

To configure LLDP:

1. Configure LLDP global configuration settings using the `config switch lldp settings` command.
2. Create LLDP profiles using the `config switch lldp profile` command to configure Type Length Values (TLVs) and other per-port settings.
3. Assign LLDP profiles to physical ports.
4. Apply VLAN to interface. (**NOTE:** LLDP profile values that are tied to VLANs will only be sent if the VLAN is assigned on the switch interface.)

a. Configure the profile.

```
show switch lldp profile Forti670i
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-signalling"
      next
    end
  set med-tlvs inventory-management network-policy
next
end
```

b. Configure the interface.

```
show switch interface port4
config switch interface
  edit "port4"
    set allowed-vlans 400
    set snmp auto
  next
end
```

c. Connect a phone with LLDP-MED capability to the interface. **NOTE: Make certain the LLDP, Learning, and DHCP features are enabled.**

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

d. Verify.

```
show switch lldp neighbor-det port4

Neighbor learned on port port4 by LLDP protocol
Last change 12 seconds ago
Last packet received 12 seconds ago
Chassis ID: 10.105.251.40 (ip)
System Name: FON-670i
System Description:
V12.740.335.12.B
Time To Live: 60 seconds
System Capabilities: BT
Enabled Capabilities: BT
MED type: Communication Device Endpoint (Class III)
MED Capabilities: CP
Management IP Address: 10.105.251.40
Port ID: 00:a8:59:d8:f1:f6 (mac)
Port description: WAN Port 10M/100M/1000M
IEEE802.3, Power via MDI:
Power devicetype: PD
PSE MDI Power: Not Supported
PSE MDI Power Enabled: No
PSE Pair Selection: Can not be controlled
PSE power pairs: Signal
Power class: 1
Power type: 802.3at off
Power source: Unknown
Power priority: Unknown
Power requested: 0
Power allocated: 0
LLDP-MED, Network Policies:
voice: VLAN: 400 (tagged), Priority: 5 DSCP: 46
voice-signaling: VLAN: 400 (tagged), Priority: 4 DSCP: 35
streaming-video: VLAN: 400 (tagged), Priority: 3 DSCP: 40
```

Checking LLDP details

Using the GUI:

Go to *Switch > Monitor > LLDP*.

LLDP OIDs

Starting in FortiSwitchOS, the following object identifiers (OIDs) are supported by the LLDP management information base (MIB) file:

- .1.0.8802.1.1.2.1.1 (IldpConfiguration)
 - IldpMessageTxInterval
 - IldpMessageTxHoldMultiplier
 - IldpReinitDelay

- IldpTxDelay
- IldpNotificationInterval
- .1.0.8802.1.1.2.1.4.1 (IldpRemoteSystemsData.IldpRemTable)
 - IldpRemChassisIdSubtype
 - IldpRemChassisId
 - IldpRemPortSubtype
 - IldpRemPortId
 - IldpRemPortDesc
 - IldpRemSysName
 - IldpRemSysDesc
 - IldpRemSysCapSupported
 - IldpRemSysCapEnabled
- .1.0.8802.1.1.2.1.4.2 (IldpRemoteSystemsData.IldpRemManAddrTable)
 - IldpRemManAddrIfSubtype
 - IldpRemManAddrIfId
 - IldpRemManAddrOID

MAC/IP/protocol-based VLANs

The FortiSwitch unit assigns VLANs to packets based on the incoming port or the VLAN tag in the packet. The MAC/IP/protocol-based VLAN feature enables the assignment of VLANs based on specific fields in an ingress packet (MAC address, IP address, or layer-2 protocol).

This chapter covers the following topics:

- [Overview on page 125](#)
- [Configuring MAC/IP/protocol-based VLANs on page 125](#)
- [Checking the configuration on page 128](#)

Overview

When a MAC/IP/protocol-based VLAN is assigned to a port, the default behavior is for egress packets with that VLAN value to include the VLAN tag. Use the `set untagged-vlans <vlan>` configuration command to remove the VLAN tag from egress packets. For an example of the command, see the [Example configuration on page 127](#).

The MAC/IP/protocol-based VLAN feature assigns the VLAN based on MAC address, IP address, or layer-2 protocol.

MAC based

In MAC-based VLAN assignment, the FortiSwitch unit associates a VLAN with each packet based on the originating MAC address.

IP based

In IP-based VLAN assignment, the FortiSwitch unit associates a VLAN with each packet based on the originating IP address or IP subnet. IPv4 is supported with prefix masks from 1 to 32. IPv6 is also supported, depending on hardware availability, with prefix lengths from 1 to 64.

Protocol based

In protocol-based VLAN assignment, the FortiSwitch unit associates a VLAN with each packet based on the Ethernet protocol value and the frame type (ethernet2, 802.3d/SNAP, LLC).

Configuring MAC/IP/protocol-based VLANs

Note the following prerequisites:

- The VLAN must be created in the FortiSwitch unit
- The VLAN needs to be allowed on the ingress port

Using the GUI:

1. Go to *Switch > VLAN*.
2. Select *Add VLAN* for a new VLAN or select *Edit* for an existing VLAN.
3. To configure a MAC-based VLAN:
 - a. Select *Add* under *Members by MAC Address*.
 - b. Enter a description and the MAC address.
4. To configure an IP-based VLAN:
 - a. Select *Add* under *Members by IP Address*.
 - b. Enter a description and the IP address.
5. Select *Add* or *Update* to save the settings.

Using the CLI:

```

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 #subnet mask must 1-32
        set description <128 byte string>
      next
    end
    config member-by-ipv6
      edit <id>
        set prefix xx:xx:xx:xx::/prefix #prefix must 1-64
        set description <128 byte string>
      next
    end
    config member-by-PROTO
      edit <id>
        set frametypes ethernet2 802.3d llc #default is all
        set protocol 0xXXXX
      next
    end
  next
end

```

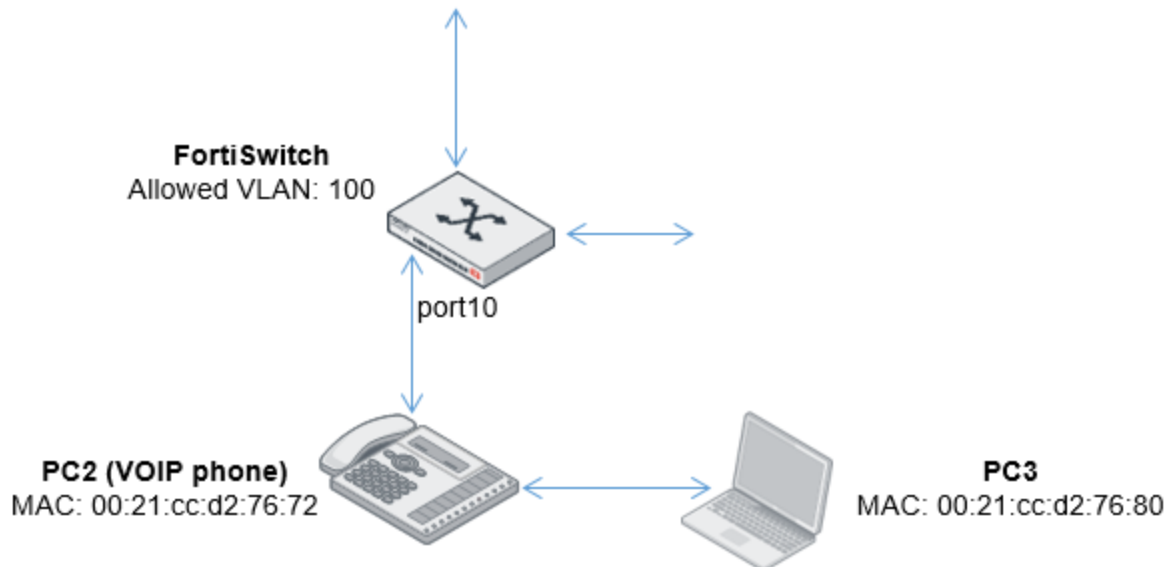
NOTE: There are hardware limits regarding how many MAC/IP/protocol-based VLANs that you can configure. If you try to add entries beyond the limit, the CLI will reject the configuration:

- Editing an existing VLAN—when you enter `next` or `end` on the `config member-by` command
- Adding a new VLAN—when you enter `next` or `end` on the `edit vlan` command
- When VLANs are defined by `config member-by-ipv4` or `config member-by-ipv6` on some FortiSwitch platforms (2xx and higher), matching ARP traffic is included in the assigned VLANs. For example, if the ARP target IP address or the ARP sender IP address match the member-by-ipv4 or member-by-ipv6 IP address, those ARP packets are included in the assigned VLANs.

Example configuration

The following example shows a CLI configuration for MAC-based VLAN where a VOIP phone and a PC share the same switch port.

In this example, a unique VLAN is assigned to the voice traffic, and the PC traffic is on the default VLAN for the port.



1. The FortiSwitch Port 10 is connected to PC2 (a VOIP phone), with MAC address 00:21:cc:d2:76:72.
2. The phone also sends traffic from PC3 (MAC= 00:21:cc:d2:76:80).
3. Assign the PC3 traffic to the default VLAN (1) on port 10.
4. Assign the voice traffic to VLAN 100.

Configure the voice 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
```

Configure switch port 10

```
config switch interface
  edit "port10"
    # allow vlan=100 on this port
```

```
# treat this as untagged on egress
set allowed-vlans 100
set untagged-vlans 100
set snmp-index 10
end
end
```

Checking the configuration

To view the MAC-based VLAN assignments, use the following command:

```
diagnose switch vlan assignment mac list sorted-by-mac

00:21:cc:d2:76:72  VLAN: 100 Installed: yes
Source: Configuration (entry 1)
Description: pc2
```

Mirroring

Packet mirroring allows you to collect packets on specified ports and then send them to another port to be collected and analyzed. All FortiSwitch models support switched port analyzer (SPAN) mode, which mirrors traffic to the specified destination interface without encapsulation.

Using remote SPAN (RSPAN) or encapsulated RSPAN (ERSPAN) allows you to send the collected packets across layer-2 domains. You can have multiple RSPAN sessions but only one ERSPAN session. In RSPAN mode, traffic is encapsulated in a VLAN. In ERSPAN mode, traffic is encapsulated in Ethernet, IPv4, and generic routing encapsulation (GRE) headers.

NOTE:

- Mirror sources cannot also be mirror destinations or members of mirror destinations if the destination is a trunk. When using RSPAN or ERSPAN in FortiLink mode, the destination ports or trunks are determined automatically (the automatically determined port can be viewed with the `diagnose switch-controller switch-info mirror status` command on the FortiGate device). The destination is often an ISL interface towards the FortiGate device. This destination can cause conflicts if the user tries to configure ports in the ISL as source ports. In the case of conflict, Fortinet recommends disabling the FortiLink traffic sniffer or omitting ports that are part of the ISL.
- Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
- When there are multiple mirror sessions in the FSW-108D-POE, FSW-224D-POE, and FSR-112D-POE models, some traffic might not be mirrored to the destination ports.

Some of the platform differences are listed in the following table:

	112D-POE	108E, 108E-FPOE, 108E-POE, 124E, 124E-FPOE, 124E-POE	124D, 224D-FPOE, 224E, 224E-POE	248D, 248E-FPOE, 248E-POE	424D, 424D-FPOE, 424D-POE	448D, 448D-FPOE, 448D-POE	524D, 524D-FPOE, 548D, 548D-FPOE 1048E	1024D 1048D 3032D 3032E
“dst” values	Ports only (can be in trunk)	Ports only (can be in trunk)	Port or trunk (no trunk members)	Port or trunk (no trunk members)	Port or trunk (no trunk members)	Port or trunk (no trunk members)	Port or trunk (no trunk members)	Port or trunk (no trunk members)
Max. sessions (active or inactive)	—	—	32	32	32	32	32	32
Max. active sessions	7	4	6	6	6	6	8	4
Max. sessions with src-egress	6	4	1	1	1	1	1	1
Max. sessions with src-ingress	6	4	4	4	4	4	4	4

	112D-POE	108E, 108E-FPOE, 108E-POE, 124E, 124E-FPOE, 124E-POE	124D, 224D-FPOE, 224E, 224E-POE	248D, 248E-FPOE, 248E-POE	424D, 424D-FPOE, 424D-POE	448D, 448D-FPOE, 448D-POE	524D, 524D-FPOE, 548D, 548D-FPOE 1048E	1024D 1048D 3032D 3032E
Max. sessions when one has src-ingress + src-egress and the rest are src-ingress	N/A	N/A	3	3	3	3	3	3
VLAN CFI and priority can be configured in RSPAN	N/A	N/A	Yes	No	Yes	No	Yes	Yes
SPAN support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RSPAN and ERSPAN support	RSPAN	No	Yes	Yes	Yes	Yes	Yes	Yes

The following topics are covered in this chapter:

- [Configuring a SPAN mirror on page 130](#)
- [Configuring an RSPAN mirror on page 133](#)
- [Configuring an ERSPAN mirror on page 134](#)

Configuring a SPAN mirror

NOTE: You can use virtual wire ports as ingress and egress mirror sources. Egress mirroring of virtual wire ports will have an additional VLAN header on all mirrored traffic.

Using the GUI:

1. Go to *Switch > Mirror*.
2. Select *Add Port Mirror*.
3. Enter a name for the mirror.
4. Select *Enabled* to set the mirror to active.
5. Select *Packet Switching When Mirroring* if the destination port is not a dedicated port. For example, enable this option if you connect a laptop to the switch and you are running a packet sniffer along with the management GUI on the laptop.
6. Select a destination port.
7. Select available ports to be used for Ingress Mirroring and Egress Monitoring.
8. Select *Add Mirror* to create the mirror.

Using the CLI:

```

config switch mirror
  edit <mirror session name>
    set mode SPAN
    set dst <interface>
    set src-egress <interface_name>
    set src-ingress <interface_name>
    set switching-packet {enable | disable}
    set status active
  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>	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. 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.	No default
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
switching-packet {enable disable}	Enable or disable the switching functionality on the dst interface when mirroring.	disable
status {active inactive}	Set the mirror session to active or inactive.	inactive

For example:

```

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

```

Multiple mirror destination ports (MTPs)

With some FortiSwitch models, you can configure multiple mirror destination ports with the following guidelines and restrictions:

- Always set the destination port before setting the src-ingress or src-egress ports.
- Any port configured as a src-ingress or src-egress port in one mirror cannot be configured as a destination port in another mirror.
- The total number of active sessions depends on your configuration.
- For switch models 124D, 124D-POE, 224D-FPOE, 248D, 248D-POE, 248D-FPOE, 224E, 224E-POE, 248E-POE, 248E-FPOE, 424D, 424D-POE, 424D-FPOE, 448D, 448D-POE, and 448D-FPOE:
 - For access control lists, you can use a mirror destination that does not have src-ingress or src-egress configured or a mirror destination that has src-ingress or src-egress configured.
- For switch models 524D, 524D-FPOE, 548D, 548D-FPOE, 1024D, 1048D, 1048E, 3032D, and 3032E:
 - For access control lists, you can use a mirror destination that does not have src-ingress or src-egress configured or a mirror destination that has src-ingress or src-egress configured.
- For switch model FSR-112D-POE:
 - You can configure up to seven mirrors, each with a different destination port.
 - Multiple ingress or egress ports can be mirrored to the same destination port.
 - An ingress or egress port cannot be mirrored to more than one destination port.

These restrictions apply to active mirrors. If you try to activate an invalid mirror configuration, the system will display the `Hardware active mirror session limit reached. Please deactivate or delete another active session to make room. error message.`

The following example configuration is valid for FortiSwitch-3032D. This configuration includes three ingress ports, one egress port, and four destination ports. The port3 ingress and egress ports are mirrored to multiple destinations.

```
config switch mirror
  edit "m1"
    set mode SPAN
    set dst "port16"
    set status active
    set src-ingress "port3" "port5" "port7"
  next
  edit "m2"
    set mode SPAN
    set dst "port22"
    set status active
    set src-ingress "port3" "port5"
  next
  edit "m3"
    set mode SPAN
    set dst "port1"
    set status active
    set src-ingress "port3"
  next
  edit "m4"
    set mode SPAN
    set dst "port2"
    set status active
    set src-egress "port3"
```

```
end
```

The following example configuration includes three ingress ports, three egress ports and four destination ports. Each ingress and egress port is mirrored to only one destination port.

```
config switch mirror
  edit "m1"
    set mode SPAN
    set dst "port1"
    set status active
    set src-ingress "port2" "port7"
  next
  edit "m2"
    set mode SPAN
    set dst "port5"
    set status active
    set src-ingress "port2"
  next
  edit "m3"
    set mode SPAN
    set dst "port3"
    set status active
    set src-ingress "port6"
  next
  edit "m4"
    set mode SPAN
    set dst "port4"
    set status active
    set src-egress "port6" "port8"
end
```

Configuring an RSPAN mirror

NOTE: RSPAN traffic crossing a switch on a VLAN configured with “RSPAN-VLAN” enabled will appear as unknown unicast, multicast, or broadcast traffic. This traffic is not exempt from storm control and might be rate limited as a result. To avoid this issue, you can dedicate a port or ports to RSPAN and then disable storm control on those ports. Non-RSPAN VLANs can be used on those ports as well, but they will not be protected by storm control.

To configure RSPAN:

```
config switch mirror
  edit <mirror session name>
    set mode RSPAN
    set dst <interface>
    set switching-packet {enable | disable}
    set src-ingress <interface_name>
    set src-egress <interface_name>
    set encap-vlan-tpid <0x0001-0xfffe>
    set encap-vlan-priority <0-7>
    set encap-vlan-cfi <0-1>
    set encap-vlan-id <1-4094>
    set status active
  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>	Set the trunk or physical port that will act as a mirror. The physical port cannot be part of a trunk.	No default
encap-vlan-cfi <0-1>	Set the canonical format identifier (CFI) or drop eligible indicator (DEI) bit in the ERSPAN or RSPAN VLAN header. NOTE: This option is not available on the 248D, 248D-POE, 248D-FPOE, 248E, 248E-POE, 248E-FPOE, 448D, 448D-POE, and 448D-FPOE models.	0
encap-vlan-id <1-4094>	Set the VLAN identifier in the ERSPAN or RSPAN VLAN header.	1
encap-vlan-priority <0-7>	Set the class of service (CoS) bits in the ERSPAN or RSPAN VLAN header. NOTE: This option is not available on the 248D, 248D-POE, 248D-FPOE, 248E, 248E-POE, 248E-FPOE, 448D, 448D-POE, and 448D-FPOE models.	0
encap-vlan-tpid <0x0001-0xfffe>	Set the tag protocol identifier (TPID) for the encapsulating VLAN header. The default value, 0x8100, is for an IEEE 802.1Q-tagged frame.	0x8100
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
switching-packet {enable disable}	Enable or disable the switching functionality on the dst interface when mirroring.	disable
status {active inactive}	Set the mirror session to active or inactive.	inactive

Configuring an ERSPAN mirror

There are two ERSPAN modes:

- ERSPAN-auto—Traffic on specified ports is mirrored to the specified destination interface using ERSPAN encapsulation. The header contents are automatically configured; you only need to specify the ERSPAN collector address.

- ERSPAN-manual—Traffic on specified ports is mirrored to the specified destination interface using ERSPAN encapsulation. You need to manually configure the header contents with layer-2 and layer-3 addresses.

To configure ERSPAN-auto:

```

config switch mirror
  edit <mirror session name>
    set mode ERSPAN-auto
    set encap-gre-protocol <hexadecimal_integer>
    set encap-ipv4-tos <hexadecimal_integer>
    set encap-ipv4-ttl <0-255>
    set encap-vlan-cfi <0-1>
    set encap-vlan-priority <0-7>
    set encap-vlan-tpid <0x0001-0xfffe>
    set erspan-collector-ip <0.0.0.1-255.255.255.255>
    set src-egress <interface_name>
    set src-ingress <interface_name>
    set strip-mirrored-traffic-tags {disable | enable}
    set status active
  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
encap-gre-protocol <hexadecimal_integer>	Set the protocol value in the ERSPAN GRE header.	0x88be
encap-ipv4-tos <hexadecimal_integer>	Set the type of service (ToS) value or enter the DSCP and ECN values in the ERSPAN IP header.	0x00
encap-ipv4-ttl <0-255>	Set the IPv4 time-to-live (TTL) value in the ERSPAN IP header.	16
encap-vlan-cfi <0-1>	Set the canonical format identifier (CFI) or drop eligible indicator (DEI) bit in the ERSPAN or RSPAN VLAN header.	0
encap-vlan-priority <0-7>	Set the class of service (CoS) bits in the ERSPAN or RSPAN VLAN header.	0
encap-vlan-tpid <0x0001-0xfffe>	Set the tag protocol identifier (TPID) for the encapsulating VLAN header. The default value, 0x8100, is for an IEEE 802.1Q-tagged frame.	0x8100
erspan-collector-ip <IPv4_address>	Required. Set the IPv4 address for the ERSPAN collector. The range is 0.0.0.1-255.255.255.255.	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

Variable	Description	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}	Enable or disable the removal of VLAN tags from mirrored traffic.	disable

To configure ERSPAN-manual:

```

config switch mirror
  edit <mirror session name>
    set mode ERSPAN-manual
    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 <0x0001-0xffff>
    set erspan-collector-ip <IPv4_address>
    set src-egress <interface_name>
    set src-ingress <interface_name>
    set strip-mirrored-traffic-tags {disable | enable}
    set switching-packet {enable | disable}
    set status active
  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>	Set the trunk or physical port that will act as a mirror. The physical port cannot be part of a trunk.	No default
encap-gre-protocol <hexadecimal_integer>	Set the protocol value in the ERSPAN GRE header.	0x88be
encap-ipv4-src <IPv4_address>	Set the IPv4 source address in the ERSPAN IP header. The range is 0.0.0.1-255.255.255.254.	0.0.0.0

Variable	Description	Default
encap-ipv4-tos <hexadecimal_integer>	Set the type of service (ToS) value or enter the DSCP and ECN values in the ERSPAN IP header.	0x00
encap-ipv4-ttl <0-255>	Set the IPv4 time-to-live (TTL) value in the ERSPAN IP header.	16
encap-mac-dst <MAC_address>	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	00:00:00:00:00:00
encap-mac-src <MAC_address>	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.	00:00:00:00:00:00
encap-vlan {tagged untagged}	Set the status of ERSPAN encapsulation headers to tagged or untagged to control whether the VLAN header is added to the encapsulated traffic.	untagged
encap-vlan-cfi <0-1>	Set the canonical format identifier (CFI) or drop eligible indicator (DEI) bit in the ERSPAN or RSPAN VLAN header. This option is available if <code>encap-vlan</code> is set to <code>tagged</code> .	0
encap-vlan-id <1-4094>	Set the VLAN identifier in the ERSPAN or RSPAN VLAN header. This option is available if <code>encap-vlan</code> is set to <code>tagged</code> .	1
encap-vlan-priority <0-7>	Set the class of service (CoS) bits in the ERSPAN or RSPAN VLAN header. This option is available when the mode is RSPAN or ERSPAN-auto. This option is available if <code>encap-vlan</code> is set to <code>tagged</code> .	0
encap-vlan-tpid <0x0001-0xffff>	Set the tag protocol identifier (TPID) for the encapsulating VLAN header. The default value, 0x8100, is for an IEEE 802.1Q-tagged frame. This option is available when the mode is RSPAN or ERSPAN-auto. This option is available if <code>encap-vlan</code> is set to <code>tagged</code> .	0x8100

Variable	Description	Default
erspan-collector-ip <IPv4_address>	Required. Set the IPv4 address for the ERSPAN collector. The range is 0.0.0.1-255.255.255.255.	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}	Enable or disable the removal of VLAN tags from mirrored traffic.	disable
switching-packet {enable disable}	Enable or disable the switching functionality on the dst interface when mirroring.	disable

Access control lists

You can use access control lists (ACLs) to configure policies for three different stages in the pipeline:

- Ingress stage for incoming traffic
- Prelookup stage for processing traffic
- Egress stage for outgoing traffic

NOTE: Before FortiSwitchOS 6.0.0, you used the `config switch acl policy` command to configure ACL policies only for the ingress stage. In FortiSwitchOS 6.0.0 and later, the `config switch acl` command has changed to specify which stage is being configured. Starting in FortiSwitchOS 6.2.0, you can create groups for multiple ingress ACLs.

This chapter covers the following topics:

- [ACL policy attributes on page 139](#)
- [Configuring an ACL policy on page 140](#)
- [Configuration examples on page 143](#)

ACL policy attributes

Key attributes of a policy include:

- **Interface.** The interface(s) on which traffic arrives at the switch. The interface can be a port, a trunk, or all interfaces. The policy applies to ingress traffic only (not egress traffic).
- **Classifier.** The classifier identifies the packets that the policy will act on. Each packet can be classified based on one or more criteria. Criteria include source and destination MAC address, VLAN id, source and destination IP address, or service (layer 4 protocol id and port number).
- **Marking** involves setting bits in the packet header to indicate the priority of this packet.
- **Actions.** If a packet matches the classifier criteria for a given ACL, the following types of action may be applied to the packet:
 - allow or block the packet, redirect the packet, mirror the packet
 - police the traffic
 - mirror the packet to another port, interface, or trunk
 - mirror the traffic
 - CoS queue assignment
 - outer VLAN tag assignment
 - egress mask to filter packets
 - specify a schedule when the ACL policy will be applied
 - make the ACL policy active or inactive

The switch uses specialized TCAM memory to perform ACL matching.

NOTE: Each model of the FortiSwitch unit provides different ACL-related capabilities. When you configure the ACL policy, the system will reject the request if the hardware cannot support it.

Configuring an ACL policy

You can configure ACL policies for each stage: ingress, egress, and prelookup.

NOTE: The order of the classifiers provided during group creation (or during an ACL update in a group when new classifiers are added) matter. Hardware resources are allocated as best fit at the time of creation, which can cause some fragmentation and segmentation of hardware resources because not all classifiers are available at all times. Because the availability of classifiers is order dependent, some allocations succeed or fail at different times. Rebooting the switch or running the `execute acl key-compaction <acl-stage><group-id>` command can help reduce the classifier resource fragmentation.

To create an ACL ingress policy:

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

To create an ACL egress policy:

```
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 src-mac <MAC_address>
  set dst-mac <MAC_address>
  set ether-type <integer>
  set src-ip-prefix <IP_address> <mask>
  set dst-ip-prefix <IP_address> <mask>
  set service <service_ID>
  set vlan-id <VLAN_ID>
  set cos <802.1Q CoS value to match>
  set dscp <DSCP value to match>
end
config action
  set count {enable | disable}
  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
```

To create an ACL prelookup policy:

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

Creating or customizing a service

Optionally, you can create or customize a service. When you create an ACL policy (ingress, egress, or prelookup), you select the service to use with the `set service <service_ID>` command under `config classifier`.

The FortiSwitch unit provides a set of pre-configured services that you can use. Use the following command to list the services:

```
show switch acl service custom
```

To create or customize a service:

```
config switch acl service custom
  edit <service name>
    set comment <string>
    set color <0-32>
    set protocol {ICMP | IP | TCP/UDP/SCTP}
    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
```

Creating a policer

Optionally, you can create a policer if you are defining ACLs to police different types of traffic. When you create an ACL policy (ingress or egress), you select the policer to use with the `set policier <policer>` command under `config action`.

To create a policer for ingress or egress traffic:

```
config switch acl policer
  edit <1-2048>
    set description <string>
    set guaranteed-bandwidth <bandwidth_value>
    set guaranteed-burst <in_bytes>
    set maximum-burst <in_bytes>
    set type {egress | ingress}
  end
```

Each policy is assigned a unique policy ID that is automatically assigned. To view it, use the `get switch acl {egress | ingress | prelookup}` command.

Viewing counters

NOTE: On the 4xxE platforms, the ACL byte counters for the prelookup stage are not available (they will always show as 0 on the CLI). The packet counters are available.

Use the following command to display the counters associated with all policies or with an ingress, egress, or prelookup policy:

```
get switch acl counters {all | egress | ingress | prelookup}
```

For example:

```
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
```

Clearing counters

Use the following command to clear the counters associated with all policies or with an ingress, egress, or prelookup policy:

```
execute acl clear-counter {all | egress | ingress | prelookup}
```

Clearing unused classifiers

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>
```

NOTE: This command currently only works on the ingress policy.

Configuration examples

Example 1

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 active
  end
```

Example 2

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-all disable
    set ingress-interface "port1"
    set status active
    config action
        set count enable
        set mirror mirror-1
    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

```

Example 3

The FortiSwitch unit can map different flows (for example, based on source and destination IP addresses) to specific outgoing ports.

In the following example, flows are redirected (based on destination IP) to different outgoing ports, connected to separate FortiDDOS appliances. This allows you to apply different FortiDDOS service profiles to different types of traffic:

```

config switch acl ingress # apply policy to port 1 ingress and send to port 3
edit 1
    config action
        set count enable
        set redirect "port3" # use redirect to shift selected traffic to new
            destination
    end
    config classifier
        set dst-ip-prefix 100.100.100.0 255.255.255.0
    end
    set description "cnt_n_mirror13"
    set ingress-interface "port1"
    set status active
next
edit 2
    config action # apply policy to port 3 ingress and send to port 1
        set count enable
        set redirect "port1"
    end
    config classifier
        set src-ip-prefix 100.100.100.0 255.255.255.0
    end
    set description "cnt_n_mirror31"
    set ingress-interface-all disable
    set ingress-interface "port3"
    set status inactive

```

```

    next
end

config switch acl ingress # apply policy to port 1 ingress and send to port 4
edit 3
    config action
        set count enable
        set redirect "port4" # use redirect to shift selected traffic to new
            destination
    end
    config classifier
        set dst-ip-prefix 20.20.20.0 255.255.255.0
    end
    set description "cnt_n_mirror14"
    set ingress-interface "port1"
    set status active
next
edit 4
    config action # apply policy to port 4 ingress and send to port 1
        set count enable
        set redirect "port1"
    end
    config classifier
        set src-ip-prefix 20.20.20.0 255.255.255.0
    end
    set description "cnt_n_mirror41"
    set ingress-interface "port4"
    set status inactive
next
end

```

Example 4

In the following example, a recurring schedule is created and then used to control when the ACL policy is active:

```

config system schedule recurring
edit schedule2
    set day monday tuesday wednesday thursday friday saturday sunday
    set start 07:00
    set end 17:00
end
config switch acl ingress
edit 1
    config action
        set remark-cos 1
        set remark-dscp 23
    end
    config classifier
        set src-mac 00:21:cc:d2:76:72
        set dst-mac d6:dd:25:be:2c:43
    end
    set ingress-interface-all enable
    set schedule schedule2
    set status active
next
end

```

Storm control

Storm control protects a LAN from disruption by traffic storms, which stem from mistakes in network configuration or denial-of-service attacks. A traffic storm, which may consist of broadcast, multicast, or unicast traffic, creates excessive traffic on the LAN and degrades network performance.

By default, storm control is disabled on a FortiSwitch unit. When enabled, it measures the data rate (in packets-per-second) for unknown unicast, unknown multicast, and broadcast traffic. You can enable and disable storm control for each of these traffic types individually. If the traffic rate for any of the types exceeds the configured threshold, the FortiSwitch unit drops the excess traffic.

By default, storm control configuration is global. Starting in FortiSwitchOS 6.2.0, you can configure storm control on a port level.

This chapter covers the following topics:

- [Configuring system-wide storm control on page 146](#)
- [Configuring port-level storm control on page 147](#)
- [Displaying the storm-control configuration on page 147](#)

Configuring system-wide storm control

If you set the rate to zero, the system drops all packets (for the enabled traffic types):

Using the GUI:

1. Go to *Switch > Storm Control*.
2. Select *Restrict Traffic*.
3. Select *Broadcast*, *Unknown Unicast*, and *Unknown Multicast* as required.
4. Select the action to take, either *Drop Packets* or *Rate Limit*.
5. If you selected *Rate Limit*, enter the number of packets per second.
6. Select *Update* to save the changes.

Using the CLI:

```
config switch storm-control
  set rate [0 | 2-10000000]
  set unknown-unicast {enable | disable}
  set unknown-mcast {enable | disable}
  set broadcast {enable | disable}
```

Configuring port-level storm control

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select a port and then select *Edit*.
3. In the Storm Control area, select *Configure Manually*.
4. Select one or more of the packet types: *Broadcast*, *Unknown Multicast*, and *Unknown Unicast*.
5. Select the action to take, either *Drop Packets* or *Rate Limit*.
6. If you selected *Rate Limit*, enter the number of packets per second.
7. Select *Update* to save the changes.

Using the CLI:

```
config switch physical-port
  edit <port_name>
    set storm-control-mode override
    config storm-control
      set broadcast {enable | disable}
      set rate [0 | 2-10000000]
      set unknown-multicast {enable | disable}
      set unknown-unicast {enable | disable}
    end
  end
end
```

Displaying the storm-control configuration

Use the following command to display the system-wide storm-control configuration:

```
get switch storm-control
```

DHCP snooping

The DHCP snooping feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. To prevent this, DHCP snooping filters messages on untrusted ports by performing the following activities:

- Validating DHCP messages received from untrusted sources and filtering out invalid messages. For example, a request to decline an DHCP offer or release a lease is ignored if the request is from a different interface than the one that created the entry.
- Building and maintaining a DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.

Other security features like dynamic ARP inspection (DAI), a security feature that rejects invalid and malicious ARP packets, also use information stored in the DHCP snooping binding database.

In the FortiSwitch unit, all ports are untrusted by default, and DHCP snooping is disabled on all untrusted ports. You indicate that a source is trusted by configuring the trust state of its connecting interface.

The FortiSwitch unit supports the option of including option-82 data in the DHCP request. (DHCP option 82 provides additional security by enabling a controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.)

For the option-82 Circuit ID field, the following format is used:

```
Circuit-ID: vlan-mod-port  
vlan - [ 2 bytes ]  
mod - [ (1 Byte) -> Snoop - 1 , Relay - 0 ]  
port - [ 1 byte ]
```

For the option-82 Remote ID field, the following format is used:

```
Remote-ID: mac [ 6 byte ]
```

For additional security, you can specify in the CLI which DHCP servers that DHCP snooping will include in the allowed server list.

This chapter covers the following topics:

- [Configuring DHCP snooping on page 148](#)
- [Checking the DHCP snooping configuration on page 152](#)
- [Removing an entry from the DHCP snooping binding database on page 153](#)

Configuring DHCP snooping

DHCP snooping is enabled per VLAN and, by default, DHCP snooping is disabled.

Configuring DHCP snooping consists of the following steps:

1. Set the DHCP snooping mode
2. Configure the VLAN settings.

3. Configure the interface settings.

Set the system-wide DHCP snooping options

Before you use DHCP snooping, select which DHCP snooping mode to use:

- Tracking mode—By default, DHCP packets coming from a DHCP server from untrusted ports are processed by the DHCP-snooping daemon. This mode is ideal when the DHCP servers need to be tracked on untrusted ports.
- Blocking mode—DHCP packets coming from a DHCP server from untrusted ports are dropped. This mode is useful when users do not want to track DHCP servers on untrusted ports.

If you want to specify which DHCP servers that DHCP snooping will include in the allowed server list, you need to enable the `dhcp-server-access-list`.

To set the system-wide DHCP snooping options:

```
config system global
  set dhcp-snoop-mode {blocking | tracking}
  set dhcp-server-access-list {enable | disable}
end
```

For example:

```
config system global
  set dhcp-server-access-list enable
end
```

Configure the VLAN settings

Using the GUI:

1. Go to *Switch > VLAN*.
2. Select *Add VLAN*.
3. Enter the VLAN identifier.
4. Enter a description for the new VLAN.
5. Enable or disable the private VLAN.
6. If you enabled the private VLAN, enter the number of isolated subVLANs and enter which subVLANs belong to the community, separated by commas or hyphens. For example, you can enter *1, 3-4, 6, 9-100*.
7. Select *DHCP Snooping*.
8. If needed, select *Verify Source Mac*, *Insert Option 82*, and *Dynamic ARP Inspection*.
9. If needed, select *IGMP Snooping*.
10. In the Members by MAC Address section, select *Add* to add a MAC address.
11. In the Members by IP Address section, select *Add* to add an IPv4 address and netmask.
12. Select *Add*.

Using the CLI:

```
config switch vlan
  edit <vlan-id>
    set dhcp-snooping enable
    set dhcp-snooping-verify-mac <enable | disable>
```

```

set dhcp-snooping-option82 <enable | disable>
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 dhcp-server-access-list
  edit <string>
    set server-ip <xxx.xxx.xxx.xxx>
  next
end
next
end

```

For example:

```

config switch vlan
  edit 10
    set dhcp-snooping enable
    config dhcp-server-access-list
      edit "list1"
        set server-ip 100.1.0.2
      next
    end
  next
end

```

NOTE: If you enable `dhcp-snooping-verify-mac`, the system will verify that the source MAC address in the DHCP request from an untrusted port matches the client hardware address.

NOTE: If you enable `dhcp-snooping-option82`, the system inserts option-82 data into the DHCP messages for this VLAN.

Configure the interface settings

After you enable DHCP snooping on a VLAN, all interfaces are in an untrusted state by default, and DHCP snooping is disabled on all untrusted interfaces. You must explicitly configure the trusted interfaces and enable DHCP snooping for each interface.

In addition, you can set a limit for how many IP addresses are in the DHCP snooping binding database for each interface by enabling the `dhcp-snoop-learning-limit-check` and setting the `learning-limit`. By default, `dhcp-snoop-learning-limit-check` is disabled, and the number of entries for an untrusted ports is 5. You can set the number of entries to 0. The maximum number of entries depends on which FortiSwitch unit you are using. For example:

```

S548DN4K16000313 # show switch vlan 1
config switch vlan
  edit 1
    set learning-limit 100
    set dhcp-snooping enable
  
```

```
    next
end
```

NOTE: If the FortiSwitch unit has already learned more IP addresses than the `dhcp-snoop-learning-limit` before the limit is set, the configuration is rejected because the FortiSwitch unit cannot select which IP addresses should be kept. If the FortiSwitch unit has learned fewer IP address or the same number of IP addresses as the `dhcp-snoop-learning-limit` before the limit is set, the configuration is accepted.

NOTE: The per-VLAN learning limit is not supported on dual-chip platforms (448 series).

Using the GUI:

1. Go to *Switch > Interface > Physical* or *Switch > Interface > Trunk*.
2. Select an interface.
3. Select *Edit*.
4. Select a *Trusted* or *Untrusted* interface for DHCP snooping.
5. If you want to accept DHCP messages with option-82 data from an untrusted interface, select the *Option-82 Trust* check box.
6. Select *OK*.

Using the CLI:

```
config switch interface / trunk
  edit <interface-name>
    set native-vlan <VLAN-ID>
    set dhcp-snooping {trusted | untrusted}
    set dhcp-snoop-learning-limit-check {enable | disable}
    set learning-limit <integer>
    set dhcp-snoop-option82-trust {enable | disable}
  next
end
```

For example:

```
config switch interface
  edit "port5"
    set native-vlan 10
    set dhcp-snooping untrusted
    set dhcp-snoop-learning-limit-check enable
    set learning-limit 7
    set dhcp-snoop-option82-trust enable
    set snmp-index 5
  next
end
```

Set `dhcp-snooping` to reflect the trust state of the interface. Where DHCP servers are located, you must configure interfaces as trusted.

If you enable `dhcp-snoop-option82-trust`, the system accepts DHCP messages with option-82 data from an untrusted interface.

Checking the DHCP snooping configuration

Use the following command to view the detailed status of DHCP snooping VLANs and ports:

```
S548DF5018000776 # get switch dhcp-snooping database-summary

snoop-enabled-vlans           :
verifysrcmac-enabled-vlans    :
option82-enabled-vlans        :
option82-trust-enabled-intfs: port5
trusted ports                  :
untrusted ports                : 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
                               port31 port32 port33 port34 port35 port36 port37 port38 port39 port40
                               port41 port42 port43 port44 port45 port46 port47 port48 port49 port50
                               port51 port52 port53 port54
Client Database                : 0 / 8000
Server Database                : 0 / 1024
Limit Database                 : 1 / 256

DHCP Global Configuration:
=====
DHCP Tracking Mode             : Tracking
DHCP Broadcast Mode            : All
DHCP Allowed Server List       : Enable
Add hostname in Option82       : Disable
```

An entry in the DHCP snooping binding database that contains an * after the IP address indicates a temporary or incomplete entry. For example:

```
08:00:27:13:16:51 2000 100.0.0.159* 10 4 port4
```

The DHCP server has not acknowledged this entry yet. If the DHCP server does not acknowledge the entry within 10 seconds, the entry is removed from the database. If the DHCP server does acknowledge the entry within 10 seconds, the entry will be considered “complete” (that is, no * after the IP address), and a proper expiration time is assigned to it.

Use the following command to view the details of the DHCP-snooping client database:

```
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
```

Use the following command to view the details of the DHCP-snooping server database:

```
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
```

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.

Removing an entry from the DHCP snooping binding database

You can remove an IP address from the DHCP snooping binding database by specifying the associated VLAN ID and MAC address:

```
execute dhcp-snooping expire-client <1-4095> <xx:xx:xx:xx:xx:xx>
```

For example:

```
execute dhcp-snooping expire-client 100 01:23:45:67:89:01
```

IP source guard

IP source guard protects a network from IPv4 spoofing by only allowing traffic on a port from specific IPv4 addresses. Traffic from other IPv4 addresses is discarded. The discarded addresses are not logged.

IP source guard allows traffic from the following sources:

- Static entries—IP addresses that have been manually associated with MAC addresses.
- Dynamic entries—IP addresses that have been learned through DHCP snooping.

By default, IP source guard is disabled. You must enable it on each port that you want protected. If you enable IP source guard and then disable it, all static and dynamic entries are removed for that interface.

There is a maximum of 2,048 IP source guard entries. When there is a conflict between static entries and dynamic entries, static entries take precedence over dynamic entries.

The following FortiSwitch models support IP source guard:

FSR-124D, FS-224D-FPOE, FS-248D, FS-424D-POE, FS-424D-FPOE, FS-448D-POE, FS-448D-FPOE, FS-424D, FS-448D, and FSW-2xxE

NOTE: IP source guard does not work with VLAN translation.

Configuring IP source guard

Configuring IP source guard consists of the following steps:

1. Enable IP source guard.
2. Configure IP source guard by binding IPv4 addresses with MAC addresses
3. Check the IP source guard entries.

Enable IP source guard

You must enable IP source guard before you can configure it.

To enable IP source guard:

```
config switch interface
  edit <port_name>
    set ip-source-guard enable
  end
```

For example:

```
config switch interface
  edit port6
    set ip-source-guard enable
  end
```

Configure IP source guard static entries

After you enable IP source guard, you can configure static entries by binding IPv4 addresses with MAC addresses. For IP source guard dynamic entries, you need to configure DHCP snooping. See [DHCP snooping on page 148](#).

To configure IP source guard:

```
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
```

For example:

```
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
```

Check the IP source guard entries

After you configure IP source guard, you can check the entries. Static entries are manually added by the `config switch ip-source-guard` command. Dynamic entries are added by DHCP snooping.

Use this command to display all IP source-guard entries:

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

Dynamic ARP inspection

Dynamic ARP Inspection (DAI) prevents man-in-the-middle attacks and IP address spoofing by checking that packets from untrusted ports have valid IP-MAC-address binding. To use DAI, you must first enable the DHCP snooping feature and then enable DAI for each VLAN. See [DHCP snooping on page 148](#).

This chapter covers the following topics:

- [Configuring DAI on page 156](#)
- [Checking ARP packets on page 157](#)

Configuring DAI

Configuring DAI consists of the following steps:

1. Enable DAI for each VLAN. By default, it is disabled.
2. Enable DAI for the switch interface. By default, all interfaces are in an untrusted state. You must explicitly configure the trusted interfaces.

Enable DAI for each VLAN

Using the GUI:

1. Go to *Switch > VLAN*.
2. Select *Add VLAN*.
3. Enter the VLAN identifier.
4. Enter a description for the new VLAN.
5. Select *DHCP Snooping*.
6. Select *Dynamic ARP Inspection*.
7. Select *Add*.

Using the CLI:

```
config switch vlan
  edit <vlan-id>
    set arp-inspection {enable | disable}
  next
end
```

Enable DAI for the switch interface

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select an interface and select *Edit*.
3. Enter the VLAN identifier.
4. Enter a description for the new VLAN.

5. Select *Untrusted* or *Trusted* for *DHCP Snooping*.
6. Select *OK*.

Using the CLI:

```
config switch interface
  edit <interface-name>
    set arp-inspection-trust <untrusted | trusted>
  next
end
```

Checking ARP packets

Use the following command to see how many ARP packets have been dropped or forwarded:

```
#diagnose switch arp-inspection stats
```

vlan 100	arp-request	arp-reply
received	0	0
forwarded	0	0
dropped	0	0

IGMP snooping

The FortiSwitch unit uses the information passed in IGMP messages to optimize the forwarding of multicast traffic.

IGMP snooping allows the FortiSwitch unit to passively listen to the Internet Group Management Protocol (IGMP) network traffic between hosts and routers. The switch uses this information to determine which ports are interested in receiving each multicast feed. The FortiSwitch unit can reduce unnecessary multicast traffic on the LAN by pruning multicast traffic from links that do not contain a multicast listener.

Essentially, IGMP snooping is a layer-2 optimization for the layer-3 IGMP.

The current version of IGMP is version 3, and the FortiSwitch unit is also compatible with IGMPv1 and IGMPv2.

Here is the basic IGMP snooping operation:

1. A host expresses interest in joining a multicast group. (Sends or responds to a join message).
2. The FortiSwitch unit creates an entry in the layer-2 forwarding table (or adds the host's port to an existing entry). The switch creates one table entry per VLAN per multicast group.
3. The FortiSwitch unit removes the entry when the last host leaves the group (or when the entry ages out).

In addition, you can configure the FortiSwitch unit to send periodic queries from all ports in a specific VLAN to request IGMP reports. The FortiSwitch unit uses the IGMP reports to update the layer-2 forwarding table.

NOTE: If you want to use IGMP snooping with an MCLAG, see "[Configuring an MCLAG with IGMP snooping](#)" on page 109.

This chapter covers the following topics:

- [Notes on page 158](#)
- [Configuring IGMP snooping on page 159](#)
- [Configuring the IGMP querier on page 163](#)
- [Configuring mRouter ports on page 163](#)

Notes

- To make well-known multicast packets, such as mDNS, flood to all ports when IGMP snooping is enabled on FSR-112D-POE, you need to make the following configuration change in FortiSwitchOS 6.2.x through 6.4.2 GA:

```
config switch igmp-snooping globals
    set flood-unknown-multicast
end
```

- You must enable the IGMP snooping function (using the `igmp-snooping enable` command) before you configure a multicast router port interface.
- On the FS-100E series, IGMP snooping can be enabled on a maximum of 6 VLANs.
- Enabling the `set flood-unknown-multicast` command and then disabling it disrupts the forwarding of unknown multicast traffic to mRouter ports for a short period, depending on the query interval, because the mRouter ports need to be relearned.

- Currently, IGMPv3 (source-specific) is not fully supported. FortiSwitchOS can identify the IGMPv3 query/report messages, but the multicast group creation and traffic replication are based on the multicast group address and VLAN only (IGMPv2 operation).
- The IGMP snooping entries are added based on multicast group MAC address.
- When IGMP snooping is enabled on a VLAN on the FSR-112D-POE model:
 - All IPv6 multicast and any non-IP multicast are forwarded to querier ports only instead of getting flooded on the VLAN. The forwarding of IPv6 to the CPU is unchanged.
 - IPv4 reserved multicast is flooded to the VLAN and not forwarded to the CPU, even if the CPU is part of the VLAN.
 - Unregistered IPv4 multicast is forwarded to querier ports only.

If IPv6 multicast and/or non-IP multicast is expected to be forwarded to any ports other than querier ports, the `igmps-flood-traffic` setting can be enabled on the required ports.

- Starting with release 6.2.2, the following snooping table limits apply:

Platform Series	IGMP Snooping Table Limit
108E and 124E	1022
112D	895
200	1022
400	1022
500	1022
1024 and 1048	1022
3032	1022

NOTE: Until FortiSwitch Release 3.5.1, the table limits were hardware only. The software limit for all platforms was 8192.

Configuring IGMP snooping

Configuring IGMP snooping consists of the following major steps:

1. Configure IGMP snooping on a global level.
2. Assign VLANs and enable IGMP snooping on the interfaces.
3. Configure IGMP snooping on the VLANs.

NOTE: IGMP snooping configured under "vlan enable" + "port based disable," does not work well; only "vlan level enable" + "port level enable" can make snooping work. So, because the port is "disabled" by default, you must enable IGMP snooping on both the VLAN and the port.

1. Configure IGMP snooping on a global level

By default, the maximum time (*aging-time*) that multicast snooping entries without any packets are kept is for 300 seconds. This value can be in the range of 15-3,600 seconds. By default, *flood-unknown-multicast* is disabled, and unregistered multicast packets are forwarded only to mRouter ports. If you enable *flood-unknown-multicast*, unregistered multicast packets are forwarded to all ports in the VLAN.

Using the CLI:

```
config switch igmp-snooping globals
  set aging-time <15-3600>
  set flood-unknown-multicast {enable | disable}
end
```

For example:

```
config switch igmp-snooping globals
  set aging-time 500
  set flood-unknown-multicast enable
end
```

2. Enable IGMP snooping on the interfaces

Enable IGMP snooping on a specified switch interface. The default is enabled.

Using the GUI:

1. Go to *Switch > Interface > Physical* or *Switch > Interface > Trunk*.
2. Select an interface.
3. Select *Edit*.
4. Select *IGMP Snooping*.
5. If needed, select *Flood Reports*, *Flood Traffic*, or both.
6. Select *OK*.

Using the CLI:

```
config switch interface
  edit <port>
    set native-vlan <vlan-id>
    set igmp-snooping {enable | disable}
    set igmps-flood-reports {enable | disable}
  next
end
```

For example:

```
config switch interface
  edit port10
    set native-vlan 30
    set igmp-snooping enable
  next
  edit port2
    set native-vlan 30
    set igmp-snooping enable
  next
```

```

edit port4
    set native-vlan 30
    set igmp-snooping enable
next
edit port6
    set native-vlan 30
    set igmp-snooping enable
next and
edit port8
    set native-vlan 30
    set igmp-snooping enable
next
end

```

Use the following command to clear the learned/configured multicast group from an interface:

```
execute clear switch igmp-snoop
```

3. Configure IGMP snooping on the VLANs

Enable IGMP snooping on a specified VLAN. The default is disabled.

You can define static groups for particular multicast addresses in a VLAN that has IGMP snooping enabled. The range of multicast addresses (`mcast-addr`) from 224.0.0.1 to 224.0.0.255 cannot be used. You can specify multiple ports in the static group, separated by a space. The trunk interface can also be included in a static group.

Starting in FortiSwitchOS 6.2.0, you can also use the CLI to enable IGMP proxy, which allows the VLAN to send IGMP reports. After you enable `igmp-proxy` on a VLAN, it will start suppressing reports and leave messages. For each multicast group, only one report is sent to the upstream interface. When a leave message is received, the FortiSwitch unit will only send the leave message to the upstream interface when there are no more members left in the multicast group. The FortiSwitch unit will also reply to generic queries and will send IGMP reports to the upstream interface.

Using the CLI:

```

config switch vlan
    edit <vlan-id>
        set igmp-snooping {enable | disable}
        set igmp-proxy {enable | disable}
        config igmp-static-group
            edit <group-name>
                set mcast-addr <multicast-address>
                set members <interface>
            next
        end
    next
end

```

For example, to configure two static groups for the same VLAN:

```

config switch vlan
    edit 30
        set igmp-snooping enable
        config igmp-static-group
            edit g239-1-1-1
                set mcast-addr 239.1.1.1
                set members port2 port5 port28
            next
        end
    next
end

```

```

    next
    edit g239-2-2-2
        set mcast-addr 239.2.2.2
        set members port5 port10 trunk-1
    next
end
next
end

```

Check the IGMP snooping configuration

Use the following command to display information about IGMP snooping:

```
# get switch igmp-snooping (globals | group | interface | static-group)
```

- **globals**: display the IGMP snooping global configuration on the FortiSwitch unit
- **group**: display a list of learned groups
- **interface**: display the configured IGMP snooping interfaces and their current state
- **static-group**: display the list of configured static groups

Display the IGMP snooping global settings:

```
FS1D243Z13000023 # get switch igmp-snooping globals
aging-time : 300
flood-unknown-multicast: disabled
```

Display the learned multicast groups:

```
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 ---
```

Display the list of configured static groups:

```
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

Configuring the IGMP querier

To use the IGMP querier, you need to configure how often IGMP queries are sent, enable the IGMP querier for a specific VLAN, and specify the address for the IGMP querier.

Use the following commands to specify how many seconds are between IGMP queries. The default is 120 seconds.

```
config switch igmp-snooping globals
  set query-interval <10-1200>
end
```

For example:

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

Use the following commands to enable the IGMP querier for a specific VLAN and specify the address that IGMP reports are sent to:

```
config switch vlan
  edit 100
    set igmp-snooping {enable | disable}
    set igmp-snooping-querier {enable | disable}
    set querier-addr <IPv4_address>
  next
end
```

For example:

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

Configuring mRouter ports

Use the following commands to configure a FortiSwitch port as an mRouter port:

NOTE: These settings are not per-VLAN, so the port will act as a querier/mRouter port for all of its associated VLANs.

```
config switch interface
  edit <port>
    set igmp-snooping enable
    set igmps-flood-reports enable
    set igmps-flood-traffic enable
  next
end
```

IPv6 router advertisement guard

IPv6-enabled routers send router advertisement (RA) messages to neighboring hosts in the local network. To prevent the spoofing of the RA messages, RA guard inspects RA messages to see if they meet the criteria contained in an RA-guard policy. If the RA messages match the criteria in the policy, they are forwarded. If the RA messages do not match the criteria in the policy, they are dropped.

The IPv6 RA-guard policy checks for the following criteria in each RA message:

- Whether it has been flagged with the M (managed address configuration) flag or O (other configuration) flag
- Whether the hop number is equal or more than the minimum hop limit
- Whether the hop number is equal or less than the maximum hop limit
- Whether the default router preference is set to high, medium, or low
- Whether the source IPv6 address matches an allowed address in an IPv6 access list (created with the `config router access-list6` command)
- Whether the IPv6 address prefix matches an allowed prefix in an IPv6 prefix list (created with the `config router prefix-list6` command)
- Whether the device is a host or a router. If the device is a host, all RA messages are dropped. If the device is a router, the other criteria in the policy are checked.

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

Configuring IPv6 RA guard

Configuring IPv6 RA guard consists of the following steps:

1. (Optional) Create lists of source IPv6 addresses and IPv6 address prefixes that are allowed in RA messages.
2. Create one or more IPv6 RA-guard policies.
3. Apply the IPv6 RA-guard policies to switch interfaces and VLANs.

Create an IPv6 access list

Create an IPv6 access list if you want to specify which source IPv6 address are allowed in RA messages. When no rule in the IPv6 access list is matched, the RA messages are dropped.

To create an IPv6 access list:

```
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
```

For example:

```
config router access-list6
  edit accesslist1
    set comments "IPv6 access list"
  config rule
    edit 1
      set action permit
      set prefix6 fe80::a5b:eff:fe1:95e5
      set exact-match disable
    next
  end
end
```

Create an IPv6 prefix list

Create an IPv6 prefix list if you want to specify which IPv6 prefixes in the RA option type 3 are allowed in RA messages. When no rule in the IPv6 prefix list is matched, the RA messages are dropped.

To create an IPv6 prefix list:

```
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
```

For example:

```
config router prefix-list6
  edit prefixlist1
    set comments "IPv6 prefix list"
  config rule
    edit 1
      set action permit
      set prefix6 any
      set ge 50
      set le 50
    next
  end
end
```

Create an IPv6 RA-guard policy

In the IPv6 RA-guard policy, you specify the criteria that RA messages must match before the RA messages are forwarded.

To create an IPv6 RA-guard policy:

```
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
```

For example:

```
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
```

Apply the IPv6 RA-guard policy

After you create an IPv6 RA-guard policy, you need to apply it to the appropriate switch ports or trunks and VLANs. You can create and apply different policies to different VLANs.

To apply the IPv6 RA-guard policy:

```
config switch interface
  edit <interface_name>
  config raguard
    edit <ID>
      set raguard-policy <name_of_RA_guard_policy>
      set vlan-list <list_of_VLANs>
    next
  end
end
```

For example:

```
config switch interface
  edit <interface_name>
  config raguard
    edit 1
      set raguard-policy RApolicy1
      set vlan-list 1
    next
    edit 2
```

```
        set rguard-policy RApolicy2
        set vlan-list 2-5
    next
end
end
```

View available IPv6 RA-guard policies

Use the following command to list the available IPv6 RA-guard policies:

```
get switch rguard-policy
```

For example:

```
S524DF4K15000024 # get switch rguard-policy
== [ RApolicy1 ]
name: RApolicy1
```

Private VLANs

A private VLAN (PVLAN) divides the original VLAN (termed the primary VLAN) into sub-VLANs (secondary VLANs), while retaining the existing IP subnet and layer-3 configuration. Unlike a regular VLAN, which is a single broadcast domain, a PVLAN partitions one broadcast domain into multiple smaller broadcast subdomains.

After a PVLAN VLAN is configured, the primary VLAN forwards frames downstream to all secondary VLANs.

There are two main types of secondary VLANs:

- **Isolated:** Any switch ports associated with an isolated VLAN can reach the primary VLAN, but not any other secondary VLAN. In addition, hosts associated with the same isolated VLAN cannot reach each other. Only one isolated VLAN is allowed in one PVLAN domain.
- **Community:** Any switch ports associated with a common community VLAN can communicate with each other and with the primary VLAN but not with any other secondary VLAN. You might have multiple distinct community VLANs within one PVLAN domain.

There are mainly two types of ports in a PVLAN: promiscuous (P-Port) and host.

- **Promiscuous Port (P-Port):** The switch port connects to a router, firewall, or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port on the VLAN.
- **Host Ports** further divides into two types – isolated port (I-Port) and community port (C-port).
 - **Isolated Port (I-Port):** Connects to the regular host that resides on isolated VLAN. This port communicates only with P-Ports.
 - **Community Port (C-Port):** Connects to the regular host that resides on community VLAN. This port communicates with P-Ports and ports on the same community VLAN.

This chapter covers the following topics:

- [Creating and enabling a PVLAN on page 168](#)
- [Configuring the PVLAN ports on page 169](#)
- [Private VLAN example on page 169](#)

Creating and enabling a PVLAN

Using the GUI:

1. Go to *Switch > VLAN*.
2. Select *Add VLAN* to create a new PVLAN.
3. Enter the VLAN identifier.
4. Enter a description for the new PVLAN.
5. Select *Enabled* to enable the new PVLAN.
6. Enter a single VLAN identifier for the isolated subVLAN.
7. If needed, enter one VLAN identifier or multiple VLAN identifiers for a common community subVLAN.
8. Select *Add*.

Configuring the PVLAN ports

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select the port to configure.
3. Select *Edit*.
4. Select if the Private VLAN port is a promiscuous port or part of a sub-VLAN.
5. For a promiscuous port, select the primary VLAN identifier.
6. For a port that is part of a sub-VLAN, select the primary VLAN identifier and the sub-VLAN identifier.
7. Select *OK*.

Private VLAN example

1. Enabling a PVLAN:

```
config switch vlan
  edit 1000
    set private-vlan enable
    set isolated-vlan 101
    set community-vlans 200-210
  end
end
```

2. Configuring the PVLAN ports:

```
config switch interface
  edit "port2"
    set private-vlan promiscuous
    set primary-vlan 1000
  next
  edit "port3"
    set private-vlan sub-vlan
    set primary-vlan 1000
    set sub-vlan 200
  next
  edit "port7"
    set private-vlan sub-vlan
    set primary-vlan 1000
    set sub-vlan 101
  next
  edit "port19"
    set private-vlan promiscuous
    set primary-vlan 1000
  next
  edit "port20"
    set private-vlan sub-vlan
    set primary-vlan 1000
    set sub-vlan 101
  next
  edit "port21"
```

```
    set private-vlan sub-vlan
    set primary-vlan 1000
    set sub-vlan 101
  end
end
```

Quality of service

Quality of service (QoS) provides the ability to set particular priorities for different applications, users, or data flows.

QoS involves the following elements:

- **Classification** is the process of determining the priority of a packet. This can be as simple as trusting the QoS markings in the packet header when it is received and so accept the packet. Alternatively, it can hinge on criteria (such as incoming port, VLAN, or service) that are defined by the network administrator.
- **Marking** involves setting bits in the packet header to indicate the priority of this packet.
- **Queuing** involves defining priority queues to ensure that packets marked as high priority take precedence over those marked as lower priority. If network congestion becomes so severe that packet drops are inevitable, the queuing process will also select the packets to drop.

The FortiSwitch unit supports the following QoS configuration capabilities:

- Mapping the IEEE 802.1p and layer-3 QoS values (Differentiated Services and IP Precedence) to an outbound QoS queue number.
- Providing eight egress queues on each port.
- Policing the maximum data rate of egress traffic on the interface.

This chapter covers the following topics:

- [Classification on page 171](#)
- [Marking on page 172](#)
- [Queuing on page 172](#)
- [Determining the egress queue on page 173](#)
- [Configuring FortiSwitch QoS on page 173](#)
- [Checking the QoS statistics on page 179](#)
- [Clearing and restoring QoS statistics on page 183](#)

Classification

The IEEE 802.1p standard defines a class of service (CoS) value (ranging from 0-7) that is included in the Ethernet frame. The Internet Protocol defines the layer-3 QoS values that are carried in the IP packet (Differentiated Services, IP Precedence). The FortiSwitch unit provides configurable mappings from CoS or IP-DSCP values to egress queue values.

Fortinet recommends that you do not enable trust for both Dot1p and DSCP at the same time on the same interface. If you do want to trust both Dot1p and IP-DSCP, the switch uses the latter value (DSCP) to determine the queue. The switch will use the Dot1p value and mapping only if the packet contains no DSCP value. For details, refer to [Determining the egress queue on page 173](#).

Marking

FortiSwitchOS supports two ways to indicate the priority of outgoing packets:

- **CoS marking:** The priority is set with the CoS value of the 802.1Q tag. The range of CoS values is 0-7.
- **Differential service code point (DSCP) marking:** The priority is set with the DSCP value in the IP header. The range of DSCP values is 0-63.

You can use one of these methods or both methods.

Whether the CoS or DSCP values of inbound packets are remarked is subject to the classification by ACL rules for the ingress interfaces. When CoS or DSCP marking take place, the outbound queuing is not impacted, meaning it is still based on trust maps and the original CoS or DSCP values, as described in [Determining the egress queue on page 173](#).

The following example shows how to use the CLI to configure an ACL policy to mark the CoS and DSCP values of inbound packets to 4 and 48 on port1 when their CoS values are 2:

```
config switch acl ingress
  edit 10
    config action
      set count enable
      set remark-cos 4
      set remark-dscp 48
    end
    config classifier
      set cos 2
    end
    set ingress-interface "port1"
    set status active
  next
end
```

Queuing

Queuing determines how queued packets on an egress port are served. Each egress port supports eight queues, and three scheduling modes are available:

- **Strict Scheduling:** 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.
- **Simple Round Robin (RR):** In round robin mode, the scheduler visits each backlogged queue, servicing a single packet from each queue before moving on to the next one. The purpose of round robin scheduling is to provide fair access to the egress port bandwidth.
- **Weighted Round Robin (WRR):** 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.

Determining the egress queue

To determine the egress queue value for the packet, the FortiSwitch unit uses the configured trust values (and mappings) on the port and the QoS/CoS fields in the packet.

Packets with DSCP and CoS values

If the port is set to trust DSCP, the switch uses this value to find the queue assignment in the DSCP map for the port.

If the port is set to trust Dot1p and **not** to trust DSCP, the switch uses the packet's CoS value to look up the queue assignment in the Dot1p map for the port.

If the port is **not** set to trust Dot1p, the switch uses the default queue 0.

Packets with a CoS value but no DSCP value

The switch ignores the trust DSCP value.

- If the port is set to trust Dot1p, the switch uses the packet's CoS value to look up the queue assignment in the Dot1p map for the port.
- If the port is **not** set to trust Dot1p, the switch uses the default queue 0.

Packets with a DSCP value but no CoS value

If the port is set to trust DSCP, the switch uses the packet's DSCP value to look up the queue assignment in the DSCP map for the port.

If the port is set to trust Dot1p but **not** to trust DSCP, the switch uses the default CoS value of the port to look up the queue assignment in the Dot1p map for the port.

If the port is **not** set to trust Dot1p, the switch uses the default queue 0.

Configuring FortiSwitch QoS



FortiSwitch uses "queue-7" for network control and critical management traffic. To avoid affecting critical network control and management traffic, do not oversubscribe queue-7 or avoid using queue-7 for data traffic when configuring QoS.

This section provides procedures for the following configuration tasks:

- [Configure an 802.1p map on page 174](#)
- [Configure a DSCP map on page 175](#)
- [Configure the QoS egress policy on page 176](#)
- [Configure the egress drop mode on page 176](#)
- [Configure the switch ports on page 177](#)
- [Configure QoS on trunks on page 178](#)

- [Configure QoS on VLANs on page 178](#)
- [Configure CoS and DSCP markings on page 179](#)

Configure an 802.1p map

Using the GUI:

1. Go to *Switch > QoS > 802.1p*.
2. Select *Add Map*.
3. Enter the name of your 802.1p map.
4. Enter a description of your 802.1p map.
5. Select the queue number for each priority.
6. Select *Add Map*.

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.

Using the CLI:

You can configure an 802.1p map, which defines a mapping between IEEE 802.1p CoS values (from incoming packets on a trusted interface) and the egress queue values.

If you want to enable priority tagging on outgoing frames, enable the `egress-pri-tagging` option. This option is disabled by default.

```
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
```

For 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` command to set a different default CoS value, ranging from 0 to 7:

```
config switch interface
```

```
edit port1
  set default-cos <0-7>
```

NOTE: The `set default-cos` 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.

Configure a DSCP map

A DSCP map defines a mapping between IP precedence or DSCP values and the egress queue values.

Using the GUI:

1. Go to *Switch > QoS > IP/DSCP*.
2. Select *Add Map*.
3. Enter the name of your DCSP map.
4. Enter a description of your DCSP map.
5. Select which queue to configure.
6. Select the differentiated services to use.
7. Select the IP precedence to use.
8. Enter the raw values to use.
9. Select *Add Map*.

Using the CLI:

```
config switch qos ip-dscp-map
  edit <ip-dscp map name>
    set description <text>
    config map
      edit <entry-name1>
        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
  end
```

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

Configure the QoS egress policy

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

A valid set of values include the following:

- min-rate (minimum rate in kbps) or min-rate-percent (minimum percentage)
- max-rate (maximum rate in kbps) or max-rate-percent (maximum percentage)
- drop policy: taildrop or random early detection
- weight value (applicable if the policy schedule is weighted)

Using the GUI:

1. Go to *Switch > QoS > Egress Policy*.
2. Select *Add Policy*.
3. Enter the name of your QoS egress policy.
4. Select the scheduling mode to use.
5. For each queue, enter a description, select the drop policy to use, and enter the minimum rate in kbps, maximum rate in kbps, weight value, and WRED slop.
6. Select *Add*.

Using the CLI:

```
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 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
```

Configure the egress drop mode

NOTE: The egress-drop-mode command is available only for the 1024/1048/3032/5xx series.

When there are too many packets going through the same egress port, you can choose whether packets are dropped on ingress or egress.

Use the following commands to set the drop mode:

```
config switch physical-port
  edit <port>
    set egress-drop-mode <disabled | enabled>
  end
```

Variable	Description
disabled	Drop packets on ingress.
enabled	Drop packets on egress.

NOTE: Because too many packets are going through the same egress port, you might want to use the pause frame for flow control on the ingress side. To see the pause frame on ingress, enable the flow control “tx” on the ingress interface and disable egress-drop-mode on the egress interface.

Configure the switch ports

You can configure the following QoS settings on a switch port or a trunk:

- trust dot1p values on ingress traffic and the dot1p map to use
- trust ip-dscp values on ingress traffic and the ip-dscp map to use. (**NOTE:** Trust the dot1p values **or** the ip-dscp values but not both.)
- an egress policy for the interface
- a default CoS value (for packets with no CoS value)

If neither of the trust policies is configured on a port, the ingress traffic is mapped to queue 0 on the egress port.

If no egress policy is configured on a port, the FortiSwitch unit applies the default scheduling mode (that is, round-robin).

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select the switch port to update and then select *Edit*.
3. Select the QoS egress policy in the *QoS Policy* drop-down list.
4. Select the 802.1p map in the *Trust 802.1p* drop-down list.
5. Select the DSCP map in the *Trust IP-DSCP* drop-down list.
6. Select *OK*.

Using the CLI:

```
config switch interface
  edit <port>
    set trust-dot1p-map <map-name>
    set trust-ip-dscp-map <map-name>
    set qos-policy < policy-name >
    set default-cos <default cos value 0-7>
  next
end
```

NOTE: The `set default-cos` 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.

Configure QoS on trunks

Configuring QoS on trunk interface follows the same configuration steps as for a switch port (configure a Dot1p/DSCP map and an egress policy).

When you add a port to a trunk, the port inherits the QoS configuration of the trunk interface. A port member reverts to the default QoS configuration when it is removed from the trunk interface.

Using the GUI:

1. Go to *Switch > Interface > Trunk*.
2. Select the trunk to update and then select *Edit*.
3. Select the QoS egress policy in the *QoS Policy* drop-down list.
4. Select the 802.1p map in the *Trust 802.1p* drop-down list.
5. Select the DSCP map in the *Trust IP-DSCP* drop-down list.
6. Select *OK*.

Using the CLI:

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
```

When you configure an egress QoS policy with rate control on a trunk interface, that rate control value is applied to each port in the trunk interface. The FortiSwitch unit does not support an aggregate value for the whole trunk interface.

NOTE: The `set default-cos` 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.

Configure QoS on VLANs

You can configure a CoS queue value for a VLAN by creating an ACL policy:

```
config switch acl ingress
  edit 1
    config action
      set cos-queue 7
      set count enable
    end
    config classifier
      set vlan-id 200
    end
    set ingress-interface "port25"
    set status active
```

```
end
```

Configure CoS and DSCP markings

You can classify a packet by matching the CoS value, DSCP value, or both CoS and DSCP values. You can also configure the action to set the CoS marking value, DSCP marking value, or both.

```
config switch acl ingress
  edit <policy-id>
    config classifier
      set cos <802.1Q CoS value to match>
      set dscp <DSCP value to match>
    end
  config action
    set remark-cos <0-7>
    set remark-dscp <0-63>
  end
```

For example:

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

Checking the QoS statistics

To check the statistics for all QoS queues, use the following command:

```
diagnose switch physical-ports qos-stats list
```

To check the statistics for QoS queues for specific ports, use the following command:

```
diagnose switch physical-ports qos-stats list <list_of_ports>
```

The output differs depending on the FortiSwitch model.

For example, for the 1xxxD, 3xxxD, and 5xxxD FortiSwitch models:

```
diagnose switch physical-ports qos-stats list 1,3,4-6
```

```
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

port3 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

port4 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
-----|-----|-----|-----|-----

```

port5 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
-----|-----|-----|-----|-----

```

port6 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

For example, for the 4xxD, 4xxD-POE, 4xxD-FPOE, 2xxD, 2xxD-POE, and 2xxD-FPOE FortiSwitch models:

```
diagnose switch physical-ports qos-stats list 1,6,48
```

port1 QoS Stats:

queue	pkts	bytes	drop pkts
0	1073	1017488	0
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	60678	7700394	0

port6 QoS Stats:

queue	pkts	bytes	drop pkts
0	104779	36489164	0
1	0	0	0
2	315	317960	0
3	0	0	0
4	0	0	0
5	267121	267121000	0
6	766734	766734000	0
7	572592	42493451	0

port48 QoS Stats:

queue	pkts	bytes	drop pkts
-------	------	-------	-----------

0		1628754		131562453		0
1		0		0		0
2		400		400400		0
3		0		0		0
4		2054967		2054967000		0
5		438759		438759000		0
6		137577		137577000		0
7		166364		72177282		0

Clearing and restoring QoS statistics

The `diagnose switch physical-ports qos-stats clear` command is supported only for the 1xxD, 3xxD, and 5xxD FortiSwitch models. The `diagnose switch physical-ports qos-stats clear` command is not available for the 4xxD, 4xxD-POE, 4xxD-FPOE, 2xxD, 2xxD-POE, or 2xxD-FPOE FortiSwitch models.

To clear the statistics for the QoS queues for all ports:

```
diagnose switch physical-ports qos-stats clear
```

To clear the statistics for the QoS queues for specified ports:

```
diagnose switch physical-ports qos-stats clear <list_of_ports>
```

To reset the QoS counters to zero (applies to all applications except SNMP) for the specified ports:

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

To restore the QoS counters to the hardware values for the specified ports:

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

For example:

```
diagnose switch physical-ports qos-stats clear 1,3,4-6
diagnose switch physical-ports qos-stats set-qos-counter-zero 2,4,7-9
diagnose switch physical-ports qos-stats set-qos-counter-revert 1,3-5,7
```

sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that may impact performance and throughput. With sFlow you can export truncated packets and interface counters. The FortiSwitch unit implements sFlow version 5 and supports trunks and VLANs.

This chapter covers the following topics:

- [About sFlow on page 184](#)
- [Configuring sFlow on page 184](#)
- [Checking the sFlow configuration on page 186](#)

About sFlow

sFlow uses packet sampling to monitor network traffic. The sFlow agent captures packet information at defined intervals and sends them to an sFlow collector for analysis, providing real-time data analysis. To minimize the impact on network throughput, the information sent is only a sampling of the data.

The sFlow collector is a central server running software that analyzes and reports on network traffic. The sampled packets and counter information, referred to as flow samples and counter samples, respectively, are sent as sFlow datagrams to a collector. Upon receiving the datagrams, the sFlow collector provides real-time analysis and graphing to indicate the source of potential traffic issues. sFlow collector software is available from a number of third-party software vendors.

Configuring sFlow

Configuration consists of the following steps:

1. Enable the sFlow agent.
2. Configure sampling information on the interfaces.

Configure sFlow agents

Use the following commands to configure an sFlow agent:

1. Set the IP address of the collector.
2. Set the collector port number, which is the destination port number in sFlow UDP packets. The default value is 6343.

Using the GUI:

1. Go to *Switch > sFlow*.
2. Select *Enable*.
3. Set the collector IP address and port number.
4. Select *Apply* to save the changes.

Using the CLI:

```
config system sflow
  set collector-ip <ip/hostname>
  set collector-port <port>
end
```

Configure the interfaces

Use the following commands to configure sFlow on a port:

- Enable sFlow on the port (by default, sFlow is disabled).
- Set the sample rate. An average of one out of `count` packets is randomly sampled. The rate ranges from 0-99999; the default is 512.
- Set the direction for capturing the traffic. sFlow can capture the ingress traffic (RX), the egress traffic (TX), or both (the default).
- Set the polling interval, which defines how often the switch sends interface counters to the collector. The range of values is 1-255 and default is 30.

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select one or more ports to update and then select *Edit*.
If you selected more than one port, the port names are displayed in the name field, separated by commas.
3. Select *Enable sFlow*.
4. Select *OK* to save the changes.

Using the CLI:

```
config switch interface
  edit <port>
    set packet-sampler {enabled | disabled}
    set packet-sample-rate <count>
    set sample-direction {rx | tx | both}
    set sflow-counter-interval <interval>
  next
end
```

For example:

```
config switch interface
  edit "port20"
    set packet-sampler enabled
    set packet-sample-rate 4
    set sflow-counter-interval 3
    set snmp-index 58
  next
end
```

NOTE: Ensure that you can use the `exec` command `ping collector_ip_address` to ping the collector from the FortiSwitch unit. Then, use the built-in sniffer to trace sFlow packets (`diag sniff packet <vlan_interface_name> "udp port 6343"`).

Checking the sFlow configuration

Use the following command to display the sFlow configuration:

```
get system sflow
```

Feature licensing

Advanced features (such as dynamic routing protocols) require a feature license.

This chapter covers the following topics:

- [About licenses on page 187](#)
- [Configuring licenses on page 187](#)

About licenses

Each feature license is tied to the serial number of the FortiSwitch unit. Therefore, a feature license is valid on one system.

Configuring licenses

Configuration consists of the following steps:

1. Check license status.
2. Add a license.

Checking the license status

Using the GUI:

1. Go to *System > Dashboard*.
2. Check which licenses are currently active.
They are listed in the Current License field of the System Information section.

Using the CLI:

```
execute license status
```

Adding a license

NOTE: Adding license keys causes the system to log you out.

Using the GUI:

1. Go to *System > Config > Licenses*.
2. Select Add License.
3. Enter your license key.
4. Select *Add*.

Using the CLI:

```
execute license add <key>
```

Removing a license**Using the GUI:**

1. Go to System > Config > Licenses.
2. Select *Delete* for the license to remove
3. Select *Delete* to acknowledge the warning.

NOTE: Deleting license keys causes the system to log you out before rebooting. You will lose all configurations related to the license.

Using the CLI:

```
execute license type <type> clear
```

Layer-3 interfaces

Fortinet data center switches support loopback interfaces and switched virtual interfaces (SVIs), both of which are described in this chapter.

This chapter covers the following topics:

- [Loopback interfaces on page 189](#)
- [Switched virtual interfaces on page 190](#)
- [Layer-3 routing in hardware on page 191](#)
- [Equal cost multi-path \(ECMP\) routing on page 192](#)
- [Bidirectional forwarding detection on page 194](#)
- [Unicast reverse-path forwarding \(uRPF\) on page 195](#)
- [IP-MAC binding on page 195](#)

Loopback interfaces

A loopback interface is a special virtual interface created in software that is not associated with any hardware interface.

Dynamic routing protocols typically use a loopback interface as a reliable IP interface for routing updates. You can assign the loopback IP address to the router rather than the IP address of a specific hardware interface. Services (such as Telnet) can access the router using the loopback IP address, which remains available independent of hardware interfaces status.

No limit exists on the number of loopback interfaces you can create.

A loopback interface does not have an internal VLAN ID or a MAC addresses and always uses a /32 network mask.

Configuring loopback interfaces

Using the GUI:

1. Go to *System > Network > Interface > Loopback*.
2. Select *Add Interface*.
3. Enter a name for the loopback interface.
4. Select *Static* for the mode and then enter the IP address and netmask in the *IP/Netmask* field.
5. Select the protocols allowed to access the loopback interface.
6. Select the administration status.
7. Select *Add*.

Using the CLI:

```
config system interface
edit "loopback"
```

```
set ip 172.168.20.1 255.255.255.255
set allowaccess ping https http ssh telnet
set type loopback
set snmp-index 28
next
end
```

Switched virtual interfaces

A switched virtual interface (or SVI) is a logical interface that is associated with a VLAN and supports routing and switching protocols.

You can assign an IP address to the SVI to enable routing between VLANs. For example, SVIs can route between two different VLANs connected to a switch (no need to connect through a layer-3 router).

Configuring a switched virtual interface

Using the GUI:

1. Go to *System > Network > Interface > VLAN*.
2. Select *Add VLAN*.
3. Enter a name for the interface.
4. Select *internal* from the *Interface* drop-down list.
5. Enter a VLAN identifier in the *VLAN ID* field.
6. Select *Static* for the mode and enter an IP address and netmask in the *IP/Netmask* field.
7. Select the administration status.
8. Select *PING*, *SSH*, and *TELNET* for the *Access* options.
9. Select *Add*.

Using the CLI:

Create a system interface. Give it an IP subnet and an associated VLAN:

```
config system interface
edit <system interface name>
set ip <IP address and mask>
set vlanid <vlan>
set allowaccess ping ssh telnet
```

Example SVI configuration

The following is an example CLI configuration for SVI static routing.

In this configuration, Server-1 is connected to switch Port1, and Server-2 is connected to switch Port2. Port1 is a member of VLAN 4000, and Port2 is a member of VLAN 2. Port1 is the gateway for Server-1, and port2 is the gateway for Server-2.

NOTE: For simplicity, assume that both port1 and port are on same switch.

1. Configure the native VLANs for Port 1 and Port 2:

```
config switch interface
edit port1
set native-vlan 4000
edit port2
set native-vlan 2
end
```

2. Create L3 system interfaces that correspond to Port 1 (VLAN 4000) and Port 2 (VLAN 2):

```
config system interface
edit vlan4000
set ip 192.168.11.1/24
set vlanid 4000
set allowaccess ping ssh telnet
next
edit vlan2
set ip 192.168.10.1/24
set vlanid 2
set allowaccess ping ssh telnet
end
```

Viewing the SVI configuration

Display the status of SVI configuration using following command:

```
show system interface [ <system interface name> ]
```

Layer-3 routing in hardware

In Release 3.3.0 and later, some FortiSwitch models support hardware-based layer-3 forwarding.

For FortiSwitch models that support Equal Cost Multi-Path (ECMP) (see [Feature matrix: FortiSwitchOS 6.2.5 on page 14](#)), forwarding for all ECMP routes is performed in hardware.

For switch models that support hardware-based layer-3 forwarding but do not support ECMP, only one route to each destination will be hardware-forwarded. If you configure multiple routes to the same destination, you can configure a priority value for each route. Only the route with highest priority will be forwarded by the hardware. If no priority values are assigned to the routes, the most recently configured route is forwarded by the hardware.

Router activity

Logging allows you to review all router activity.

NOTE: Router logs are available only on supported platforms if you have the advanced features license.

To enable router logging:

1. Go to *Log > Config*.
2. Under *Event Logging*, select *Enable* and *Router*.
3. Select *Apply*.

To view router logs:

1. Go to *Log > Event Log > Router*.
2. Select *Download Router Log* to review the entries offline.

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

Configuring ECMP

The switch automatically uses ECMP to choose between equal-cost routes.

This configuration value is system-wide. The source IP address is the default value.

Notes and Restrictions

When you configure a static route with a gateway, the gateway must be in the same IP subnet as the device. Also, the destination subnet cannot match any of device IP subnets in the switch.

When you configure a static route without a gateway, the destination subnet must be in the same IP subnet as the device.

Using the CLI:

```
config system settings
  set v4-ecmp-mode [ source-ip-based ] [ dst-ip-based ] [ port-based ]
end
```

Example ECMP configuration

The following is an example CLI configuration for ECMP forwarding.

In this configuration, ports 2 and 6 are routed ports. Interfaces I-RED and I-GREEN are routed VLAN interfaces. The remaining ports in the switch are normal layer-2 ports.

1. Configure native VLANs for ports 2, 6, and 9. Also configure the “internal” interface to allow native VLANs for ports 2, 6, and 9:

```
config switch interface
  edit port2
    set native-vlan 10
  edit port6
    set native-vlan 20
```

```
edit port9
  set native-vlan 30
edit internal
  set allowed-vlans 10,20,30
end
```

2. Configure the system interfaces:

```
config system interface
edit "internal"
  set type physical
next
edit "i-blue"
  set ip 1.1.1.1 255.255.255.0
  set allowaccess ping https http ssh snmp telnet
  set vlanid 10
  set interface internal
next
edit "i-red"
  set ip 172.16.11.1 255.255.255.0
  set allowaccess ping ssh telnet
  set vlanid 20
  set interface internal
next
edit "i-green"
  set ip 172.168.13.1 255.255.255.0
  set allowaccess ping https http ssh snmp telnet
  set vlanid 30
  set interface internal
next
end
```

3. Configure static routes. This code configures multiple next-hop gateways for the same network:

```
config router static
edit 1
  set device "mgmt"
  set gateway 10.105.0.1
  set status enable
next
edit 2
  set device "i-red"
  set dst 8.8.8.0/24
  set gateway 172.16.11.2
  set status enable
next
edit 3
  set device "i-green"
  set dst 8.8.8.0/24
  set gateway 172.168.13.2
  set status enable
next
```

Viewing ECMP configuration

Display the status of the ECMP configuration using following command:

```
show system interface [ <system interface name> ]
```

Bidirectional forwarding detection

FortiSwitchOS v3.4.2 and later supports static bidirectional forwarding detection (BFD), a point-to-point protocol to detect faults in the datapath between the endpoints of an IETF-defined tunnel (such as IP, IP-in-IP, GRE, and MPLS LSP/PW).

BFD defines demand mode and asynchronous mode operation. The FortiSwitch unit supports asynchronous mode. In this mode, the systems periodically send BFD control packets to one another, and if a number of those packets in a row are not received by the other system, the session is declared to be down.

BFD packets are transported using UDP/IP encapsulation and BFD control packets are identified using well-known UDP destination port 3784 (**NOTE:** BFD echo packets are identified using 3785).

BFD packets are not visible to the intermediate nodes and are generated and processed by the tunnel end systems only.

Configuring BFD

Use the following steps to configure BFD:

1. Configure the following values in the system interface:
 - *Enable BFD:* Set to *enable* or set to *global* to inherit the global configuration value.
 - *Desired min TX interval:* This is the minimum interval that the local system would like to use between transmission of BFD control packets. Value range is 200 ms – 30,000 ms. Default value is 250.
 - *Required min RX interval:* This is the minimum interval that the local system can support between receipt of BFD control packets. If you set this value to zero, the remote system will not transmit BFD control packets. The value range is 200 ms – 30000 ms. The default value is 250.
 - *Detect multi:* This is the detection time multiplier. The negotiated transmit interval multiplied by this value is the Detection Time for the receiving system. The value range is 1 – 20. The default is 3.
2. Enable BFD in the static router configuration.

Using the CLI:

```
config system interface
  edit <system interface name>
    set bfd {enable| disable | global}
    set bfd-desired-min-tx <number of ms>
    set bfd-required-min-rx <number of ms>
    set bfd-detect-multi [1..20]
  next
config router static
  edit 1
    set bfd enable
    set status enable
```

Viewing BFD configuration

Display the status of BFD sessions using following command:

```
get router info bfd neighbor [ <IP address of 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
```

Use the following command to display additional details:

```
get router info bfd neighbor detail
```

Unicast reverse-path forwarding (uRPF)

RPF, also called anti-spoofing, prevents an IP packet from being forwarded if its source IP address does not belong to a locally attached subnet (local interface) or is not part of the routing between the FortiSwitch unit and another source (such as a static route, RIP, OSPF, or BGP).

In unicast RPF, the router not only looks up the destination information but it also looks up the source information to ensure that it exists. If no source is found, that packet is dropped because the router assumes it is an error or an attack on the network.

There are two uRPF modes:

- **Strict**—The packet must be received on the same interface that the router uses to forward the return packet. In this mode, asymmetric routing paths in the network might cause legitimate traffic to be dropped.
- **Loose**—The routing table must include the source IP address of the packet. If you disable the `src-check-allow-default` option, the packet is dropped if the source IP address is not found in the routing table. If you enable the `src-check-allow-default` 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.

Configuring uRPF

By default, uRPF is disabled. You must enable it on each interface that you want protected.

```
config system interface
  edit <interface_name>
    set src-check {disable | loose | strict}
    set src-check-allow-default {enable | disable} // This option is available only
      when src-check is set to loose.
  end
```

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

Configuring IP-MAC binding

Use the following steps to configure IP-MAC binding:

1. Enable the IP-MAC binding global setting.
2. Create the IP-MAC bindings. You can activate each binding individually.
3. Set each port to follow the global setting. You can also override the global setting for individual ports by enabling or disabling IP-MAC binding for the port.

Using the GUI:

Create the IP-MAC binding:

1. Go to *Switch > IP MAC Binding*.
2. Select *Add IP MAC Binding* to create a new binding.
3. Select *Status*.
4. Enter the IP address and netmask.
5. Enter the MAC address.
6. Select *Add*.

Using the CLI:

```
config switch global
    set ip-mac-binding [enable| disable]

config switch ip-mac-binding
    edit 1
        set ip <IP address and network mask>
        set mac <MAC address>
        set status (enable| disable)
    next
end
config switch interface
    edit <port>
        set ip-mac-binding (enable| disable | global)
    edit <trunk name>
        set ip-mac-binding (enable| disable | global)
```

Notes

For a switch port, the default IP-MAC binding value is disabled.

When you configure a trunk, the trunk follows the global value by default. You can also explicitly enable or disable IP-MAC binding for a trunk, as shown in the CLI configuration.

When you add member ports to the trunk, all ports take on the trunk setting. If you later remove a port from the trunk group, the port is reset to the default value (disabled).

No duplicate entries are allowed in the mapping table.

Rules are disabled by default. You need to explicitly enable each rule.

The mapping table holds up to 1024 rules.

Viewing IP-MAC binding configuration

Display the status of IP-MAC binding using the following command:

```
show switch ip-mac-binding <entry number>
```

DHCP server and relay

A DHCP server provides an address, from a defined address range, to a client on the network that requests it.

You can configure one or more DHCP servers on any FortiSwitch interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.

You can configure a FortiSwitch interface as a DHCP relay. The interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have the appropriate routing so that its response packets to the DHCP clients arrive at the unit.

NOTE:

- DHCP snooping and the DHCP server can be enabled at the same time.
- The DHCP server and DHCP relay cannot be enabled at the same time.

This chapter covers the following topics:

- [Configuring a DHCP server on page 198](#)
- [Detailed operation of a DHCP relay on page 201](#)
- [Configuring a DHCP relay on page 202](#)

Configuring a DHCP server

NOTE: The 4xx, 5xx, 1xxx, and 3xxx models support configuring DHCP servers. The following table lists the maximum number of clients for the supported FortiSwitch models:

FortiSwitch models	Maximum number of clients
4xx	15,000
5xx	20,000
1024D, 1048D, 3032D	30,000
1048E, 3032E	50,000

To configure a DHCP server:

```
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>
next
end

```

For example:

```

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
```

Configuring the IP address range

By default, the FortiSwitch unit assigns an address range based on the address of the interface for the complete scope of the address. For example, if the interface address is 172.20.120.230, the default range created is 172.20.120.231 to 172.20.120.254.

To configure the IP address range:

```
config system dhcp server
  edit <id>
    config ip-range
      edit <id>
        set end-ip <xxx.xxx.xxx.xxx>
        set start-ip <xxx.xxx.xxx.xxx>
      next
    end
  next
end
```

Assigning IP settings to specific MAC addresses

If you want the DHCP server to assign IP settings to specific MAC addresses, you need to reserve the IP addresses.

To assign IP settings to specific MAC addresses:

```
config system dhcp server
  edit <id>
    config reserved-address
      edit <id>1
        set action {assign | block | reserved}
        set description <string>
        set ip <xxx.xxx.xxx.xxx>
        set mac <xx:xx:xx:xx:xx:xx>
        set type {mac | option82}
      next
    end
  next
end
```

Configuring DHCP custom options

The DHCP server maintains a table for the potential options. The FortiSwitch DHCP server supports up to a maximum of 30 custom options.

To configure the DHCP custom options:

```
config system dhcp server
  edit <id>
    config options
      edit <id>
        set code <integer>
        set ip <IP_addresses>
      next
    end
  next
end
```

```

        set type {fqdn | hex | ip | string}
        set value <string>
    next
end
next
end

```

Excluding addresses in DHCP

If you have a large address range for the DHCP server, you can block a range of addresses that will not be included in the available addresses for the connecting users.

To exclude addresses in DHCP:

```

config system dhcp server
  edit <id>
    config exclude-range
      edit <id>
        set end-ip <xxx.xxx.xxx.xxx>
        set start-ip <xxx.xxx.xxx.xxx>
      next
    end
  next
end

```

Listing DHCP leases

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. Use one of the following commands to check the DHCP leases:

```

execute dhcp lease-list
execute dhcp lease-list <interface>

```

Breaking DHCP leases

If you need to end an IP address lease, you can break the lease. This is useful if you have limited addresses and longer lease times when some leases are no longer necessary, for example, with corporate visitors. Use one of the following commands to break the DHCP leases:

```

execute dhcp lease-clear all
execute dhcp lease-clear <xxx.xxx.xxx.xxx,yyy.yyy.yyy.yyy,...>

```

Detailed operation of a DHCP relay

DHCP relay operates as follows:

1. DHCP client C broadcasts a DHCP/BOOTP discover message on its subnet.
2. The relay agent examines the gateway IP address field in the DHCP/BOOTP message header. If the field has an IP address of 0.0.0.0, the agent fills it with the relay agent's or router's IP address and forwards the message to the remote subnet of the DHCP server.

3. When DHCP server receives the message, it examines the gateway IP address field for a DHCP scope that can be used by the DHCP server to supply an IP address lease.
4. If DHCP server has multiple DHCP scopes, the address in the gateway IP address field (GIADDR) identifies the DHCP scope from which to offer an IP address lease.
5. DHCP server sends an IP address lease offer (DHCPOFFER) directly to the relay agent identified in the gateway IP address (GIADDR) field.
6. The router then relays the address lease offer (DHCPOFFER) to the DHCP client.

NOTE:

- DHCP relay service supports up to 8 relay targets per interface.
- Each target is sent a copy of the DHCP message.

Configuring a DHCP relay

You can configure a DHCP relay on any layer-3 interface.

Using the GUI:

1. Go to *System > Network > Interface > Physical*.
2. Select *Edit* for an interface.
3. Select *Enabled* under *DHCP Relay*.
4. Enter the IP addresses for the relay servers, separated by a space.
5. If you want to include Option-82 data, select *Option-82*.
6. Select *Update*.

Using the CLI:

```
config system interface
  edit <interface-name>
    set dhcp-relay-service (enable | disable)
    set dhcp-relay-ip <ip-address1> [<ip-address2> ... <ip-address8>]
    set dhcp-relay-option82 (enable | disable)
  next
end
```

In the following example, the DHCP server has address 192.168.23.2:

```
config system interface
  edit "v15-p15"
    set dhcp-relay-service enable
    set dhcp-relay-ip "192.168.23.2" -> the DHCP server address
    set ip 192.168.15.1 255.255.255.0 -> the DHCP client subnet
    set allowaccess ping ssh snmp telnet set snmp-index 53
    set vlanid 15
    set interface "internal"
  next
end
```

OSPF routing

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

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

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

The main benefit of OSPF is that it detects link failures in the network quickly and converges network traffic successfully within seconds without any network loops. Also, OSPF has features to control which routes are propagated to contain the size of the routing tables.

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

The FortiSwitch unit supports the following capabilities:

- Support for OSPFv2.
- OSPF neighbors support authentication
- Supports NSSA
- Supports BFD
- Supports stub area
- Network scaling

NOTE: OSPF MIBs are not supported in this release.

For additional information about OSPF routing, see the [OSPF section of the FortiOS Handbook](#).

This chapter covers the following topics:

- [Terminology on page 203](#)
- [How OSPF works on page 204](#)
- [Configuring OSPF on page 205](#)

Terminology

Link State: Information is shared between directly connected routers. This information propagates throughout the network unchanged and is also used to create a shortest path first (SPF) tree.

Autonomous System (AS): A network under a common network administration.

Area: You can divide a large network into areas to limit the number of link-state updates.

Cost: The routing metric used by OSPF. Lower costs are always preferred. You can configure the cost or use the interface default.

Router ID: Each OSPF router requires a unique router ID. For the FortiSwitch unit, the unique router ID must be assigned manually.

Adjacency: When two OSPF routers have exchanged information and have the same topology table.

Topology Table: Also called the link-state table. This table contains information about every link in the network. The SPF algorithm uses the link-state information to calculate the best route to each destination.

Designated Router (DR): This router is responsible for ensuring adjacencies between all neighbors on a multi-access network (such as Ethernet). This ensures all routers do not need to maintain full adjacencies with each other. The DR is selected based on the router priority. In a tie, the router with the highest router ID is selected.

Backup DR: A backup router designed to perform the same functions in case the DR fails.

Link-State Advertisement (LSA): The method used by each router to share its routing topology with other routers in the same area.

Area Border Router (ABR): Router located on the border of one or more OSPF areas that connects those areas to the backbone area.

AS Boundary Router (AS BR): ABR located between an OSPF autonomous system and a non-OSPF network.

How OSPF works

Areas

An OSPF implementation consists of one or more areas. An area consists of a group of contiguous networks. If you configure more than one area, Area Zero is always the backbone area. An ABR links one or more areas to the OSPF backbone area.

The FortiSwitch unit supports different types of areas—stub areas, Not So Stubby areas (NSSA), and regular areas. A stub area is an interface without a default route configured. NSSA is a type of stub area that can import AS external routes and send them to the backbone but cannot receive AS external routes from the backbone or other areas. All other areas are considered regular areas.

Adjacencies

When an OSPF router boots up, it sends OSPF Hello packets to find neighbors on the same network. Neighbors exchange information, and the Link State databases of both neighbors are synchronized. At this point, these neighbors are said to be adjacent.

For two OSPF routers to become neighbors, the following conditions must be met:

- The subnet number and subnet mask for the interface must match in both routers.
- The Hello interval and Dead interval values must match.
- The routers must have the same OSPF area ID.
- If authentication is used, they must pass authentication checks.

In OSPF, routing protocol packets are only passed between adjacent routers.

Configuring OSPF

Using the GUI:

1. Create a switched virtual interface. See [Configuring a switched virtual interface on page 190](#).
2. Go to *Router > Config > OSPF > Settings*.
 - Enter a unique 32-bit number in dotted decimal format for the router identifier. **NOTE:** Without a router identifier, OSPF routing will not work.
 - If you are going to advertise default routes within OSPF, configure the default route option and enter the metric (cost) for other routing protocols.
 - If you want to redistribute non-OSPF routes, select *Connected*, *Static*, or *RIP*.
 - Select *Update*.
3. Go to *Router > Config > OSPF > Areas* and select *Add OSPF Area*.
 - Enter the area IP address.
 - Select if the area is a stub area, NSSA, or a regular area.
 - Select *Add*.
4. Go to *Router > Config > OSPF > Networks* and select *Add Network*.
 - Enter the network identifier.
 - Enter the IP address and netmask, separated with a space. Use an IP address that includes the switched virtual interface.
 - Select the area that you created.
 - Select *Add*.
5. Go to *Router > Config > OSPF > Interfaces* and select *Configure OSPF Interface*.
 - Enter a descriptive name for the OSPF interface name.
 - Select the same type of authentication that you selected for the area.
 - If you want static bidirectional forwarding detection, select *Enable* or *Global*.
 - Enter the maximum transmission unit.
 - Enter the cost.
 - Enter the number of seconds between Hello packets being sent.
 - Enter the number of seconds that a Hello packet is not received before the OSPF router decides that a neighbor has failed.
 - Select *Add*.

Using the CLI:

Configuring OSPF on the FortiSwitch unit includes the following major steps:

1. Enter the OSPF configuration mode.
2. Set the router identifier. Each router must have a unique 32-bit number. **NOTE:** Without a router identifier, OSPF routing will not work.
3. Create an area. You must create at least one area.
4. Configure the network. Attach one or more networks to each area.
5. Configure an interface to a peer OSPF router.
6. Redistribute non-OSPF routes. Advertise these non-OSPF routes within OSPF.

1. Enter the OSPF configuration mode

Enter the OSPF configuration mode to access all of the OSPF configuration commands:

```
# config router ospf
```

2. Set the router identifier

Each router within an area must have a unique 32-bit number. The router identifier is written in dotted decimal format, but it is not an IPv4 address. **NOTE:** Without a router identifier, OSPF routing will not work.

```
set router-id <router-id>
```

For example:

```
# config router ospf
(ospf) # set router-id 1.1.1.2
```

3. Create an area

You must create at least one area. The area number is written in dotted decimal format (for example, configure area 100 as 0.0.0.100).

```
config area
  edit <area number>
    set shortcut (default | disable | enable)
    set type {nssa | regular | stub}
end
```

For example:

```
(ospf) # config area
(area) # edit 0.0.0.4
(0.0.0.4) # set type nssa
```

4. Configure the network

Use this subcommand to identify the OSPF-enabled interfaces. The prefix length in the interface must be equal or larger than the prefix length in the network statement.

```
config network
  edit <network number>
    set area <area>
    set prefix <network prefix> <mask>
```

For example:

```
(ospf) # config network
(network) # edit 1
(1) # set area 0.0.0.4
(1) # set prefix 10.1.1.0 255.255.255.0
```

5. Configure the OSPF interface

Configure interface-related OSPF settings. Enter a descriptive name for the OSPF interface name. Use the `set interface` command to apply this configuration to a FortiSwitch interface:

```
config ospf-interface
```

```
edit <ospf interface name>
  set interface <interface name>
  set priority <>
```

For example:

```
(ospf) # config ospf-interface
(ospf-interface) # edit oil
(oil) # set interface vlan40-p4
(oil) # set priority 255
```

NOTE: The following values must match for an adjacency to form:

- area type and number
- interface subnet and mask
- hello interval
- dead interval

6. Redistribute non-OSPF routes

Redistribute non-OSPF routes (directly connected or static routes) within OSPF:

```
config redistribute { <name> | connected | rip | static }
  set status enable
  set metric <integer>
  set metric-type {1 | 2}
end
```

For example:

```
(ospf) # config redistribute connected
(connected) # set status enable
```

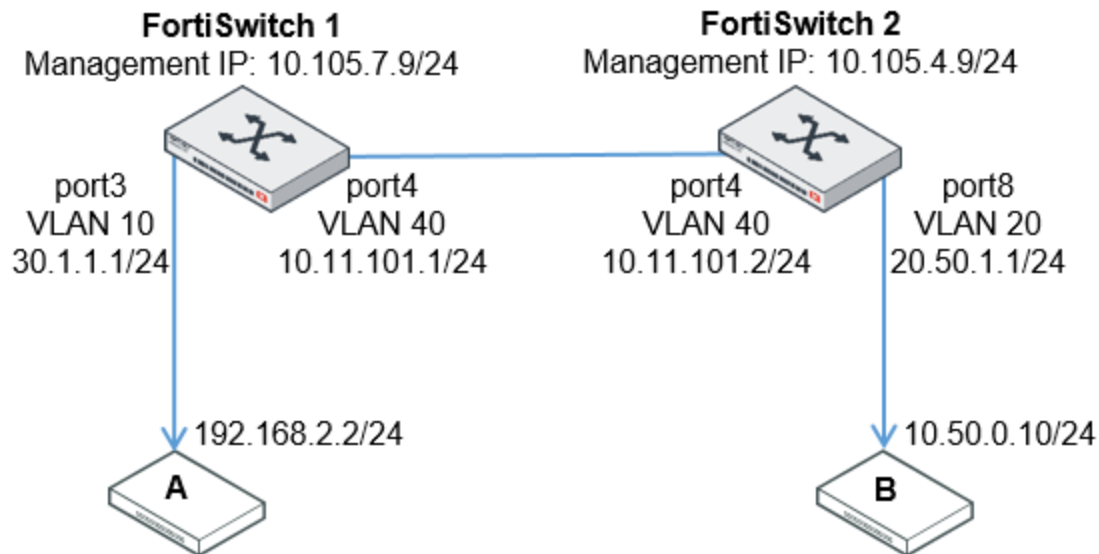
Check the OSPF configuration

The `get router info ospf` command has options to display different aspects of the OSPF configuration and status. For example:

```
get router info ospf neighbors
get router info ospf database
```

Example configuration

The following example shows a very simple OSPF network with one area. FortiSwitch 1 has one OSPF interface to FortiSwitch 2:



Configure system interfaces

These are the same configuration steps as for static routing.

Switch 1

```

config system interface
  edit vlan10-p3
    set ip 30.1.1.1 255.255.255.0
    set allowaccess ping https http ssh telnet
    set vlanid 10
  next
  edit vlan40-p4
    set ip 10.11.101.1 255.255.255.0
    set allowaccess ping https http ssh telnet
    set vlanid 40
end
config switch interface
  edit "port3"
    set native-vlan 10
  next
  edit "port4"
    set native-vlan 40
  next
end

```

Switch 2

```
config system interface
  edit vlan20-p8
    set ip 20.50.1.1 255.255.255.0
    set allowaccess ping https http ssh telnet
    set vlanid 20
  next
  edit vlan40-p4
    set ip 10.11.101.2 255.255.255.0
    set allowaccess ping https http ssh telnet
    set vlanid 40
end
config switch interface
  edit "port8"
    set native-vlan 20
  next
  edit "port4"
    set native-vlan 40
  next
end
```

Configure the OSPF router

Configure OSPF with the following:

1. Set the router ID.
2. Create the area.
3. Create the network (set network prefix and associate with an area).
4. Configure the OSPF interface.
5. Redistribute the routes.

Switch 1

```
config router ospf

  set router-id 10.11.101.1

config area
  edit 0.0.0.0
  next
end

config network
  edit 1
    set area 0.0.0.0
    set prefix 10.11.101.0 255.255.255.0
  next
end

config interface
  edit vlan40
    set cost 100
    set priority 100
  next
```

```
end

config redistribute connected
  set status enable
end

end
```

Switch 2

```
config router ospf
  set router-id 10.11.101.2

  config area
    edit 0.0.0.0
      next
    end

  config network
    edit 1
      set area 0.0.0.0
      set prefix 10.11.101.0 255.255.255.0
      next
    end

  config interface
    edit vlan40
      set cost 100
      set priority 100
      next
    end

  config redistribute connected
    set status enable
  end

end
```

Verify OSPF neighbors

```
get router info ospf neighbor all
```

Verify OSPF routes

```
get router info ospf route
```

RIP routing

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

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

The FortiSwitch unit supports RIP version 1 and RIP version 2:

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

RIP uses three timers:

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

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

When you configure RIP routing, you can choose the strategy the access list uses to permit or deny IP addresses:

- *Prefix*—Specify the IP address and bit mask to allow or block.
- *Wildcard*—Specify the Cisco-style filter to allow or block.

For additional information about RIP routing, see the [Routing Information Protocol \(RIP\) section of the FortiOS Handbook](#).

This chapter covers the following topics:

- [Terminology on page 211](#)
- [Configuring RIP routing on page 212](#)

Terminology

Access list: A list of IP addresses and the action to take for each one. Access lists provide basic route and network filtering.

Active RIP interface: Each RIP router sends and receives updates by actively communicating with its neighbors.

Keychain: A list of one or more authentication keys including its lifetime, which is how long each key is valid.

Metric: RIP uses hop count as the metric for choosing the best route. A hop count of 1 represents a network that is connected directly to the FortiSwitch unit. A hop count of 16 represents a network that cannot be reached.

Passive RIP interface: The RIP router listens to updates from other routers but does not send out updates. A passive RIP interface reduces network traffic.

Prefix list: A more powerful prefix-based filtering mechanism. A prefix is an IP address and netmask.

Split horizon: A way to avoid routing loops.

Configuring RIP routing

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

To add a new keychain using the CLI:

```
config router key-chain
  edit <keychain identifier>
  next
end
```

Using the GUI and the prefix strategy:

1. Create a switched virtual interface (SVI). See [Configuring a switched virtual interface on page 190](#).
2. Go to *Router > Config > RIP > Settings*

RIP Settings

RIP Version 1 2

Bidirectional Forwarding Detection

Default Route

Default Information Originate

Metric (1-16)

Redistribute

Connected

Static

OSPF

Timers

Update (Seconds)	<input type="text" value="30"/>	(5-2147483647)
Timeout (Seconds)	<input type="text" value="180"/>	(5-2147483647)
Garbage (Seconds)	<input type="text" value="120"/>	(5-2147483647)

[Update](#)

- Select whether you want to use RIP version 1 or RIP version 2. RIP version 2 is the default.
- If you want to use a default route, select *Default Information Originate*.
- If you want to use BFD, select *Bidirectional Forwarding Detection*.
- If you are going to advertise non-RIP routes within RIP, enter the metric (cost) for other routing protocols.
- If you want to redistribute non-RIP routes, select *Connected*, *Static*, or *RIP* and then enter the metric to use.
- If you want to change the default timer values, enter the number of seconds in the *Update*, *Timeout*, and *Garbage* fields.

- Go to *Router > Config > Access Lists* and select *Add Access List*.

Add Access List

ID ?
This value is required.

Strategy Prefix

Comments

Cancel Add

- Enter an identifier with one or more alphabetic characters.
- Enter an optional description of the access list.
- Select *Add*.
- Select *Config Rules* in the row for the access list that you just created.

Config Access List Rules

ID 1a

Strategy Prefix

Comments

Rules

ID(1-65535)	Action	Prefix	Exact Match	Manage

+ Add Rule

Cancel Update

- Select *Add Rule*.
- Enter an identifier (1-65535), select *Deny* or *Permit* to specify if the rule will block or allow the specified IP addresses, and enter the prefix.
- If you entered the complete IP address, select the *Exact Match* checkbox.
- Select *Add Rule* if you want to add more rules.
- After you have added all of the rules that you want in the access list, select *Update* to save the rules you added.

- Go to *Router > Config > RIP > Distances* and select *Add RIP Distance*.

Add RIP Distance

Distance ID	<input type="text"/>	(0-4294967295)
	This value is required.	
Distance	<input type="text"/>	(1-255)
	This value is required.	
Access List	<input type="text" value="None"/>	
IP/Netmask	<input type="text" value="0.0.0.0/0.0.0.0"/>	
	<input type="button" value="Cancel"/>	<input type="button" value="Add"/>

- Enter the distance identifier in the Distance ID field.
 - Enter the distance.
 - Select the access list that you added in the previous step.
 - Enter the IP address and netmask, separated with a space or with a slash. For example, enter `1.2.3.4/5` or `1.2.3.4 248.0.0.0`.
 - Select *Add*.
- Go to *Router > Config > RIP > Networks* and select *Add Network*.

Add RIP Network

Network ID	<input type="text"/>	(1-2147483647)
	This value is required.	
IP/Netmask	<input type="text"/>	
	This value is required.	
	<input type="button" value="Cancel"/>	<input type="button" value="Add"/>

- Enter an IP address and netmask for your RIP network, separated with a slash, and select *Add*. For example, enter `172.168.200.0/255.255.255.0`. **NOTE:** Select an IP address for a network that includes all SVIs that you want to use. You can configure multiple network ranges to cover all SVIs that will be using RIP routing.

6. Go to *Router > Config > RIP > Interfaces* and select *Configure RIP* for the appropriate interface.

Add RIP Interface

Interface	internal
Send Version	Global ▼
Receive Version	Global ▼
Passive Interface	<input type="checkbox"/>

Authentication

Authentication	<input checked="" type="radio"/> None
	<input type="radio"/> Text
	<input type="radio"/> MD5

- If you want to change the RIP version used to send and receive routing updates, select from the *Send Version* and *Receive Version* drop-down menus.
- If you do not want to send RIP updates from this interface, select *Passive Interface*.
- If you want to use authentication, select *Text* or *MD5*.
- Select *Add*.

Using the GUI and the wildcard strategy:

1. Create a switched virtual interface (SVI). See [Configuring a switched virtual interface on page 190](#).
2. Go to *Router > Config > RIP > Settings*.

RIP Settings

RIP Version 1 2

Bidirectional Forwarding Detection

Default Route

Default Information Originate

Metric (1-16)

Redistribute

Connected

Static

OSPF

Timers

Update (Seconds) (5-2147483647)

Timeout (Seconds) (5-2147483647)

Garbage (Seconds) (5-2147483647)

Update

- Select whether you want to use RIP version 1 or RIP version 2. RIP version 2 is the default.
- If you want to use a default route, select *Default Information Originate*.
- If you want to use BFD, select *Bidirectional Forwarding Detection*.
- If you are going to advertise non-RIP routes within RIP, enter the metric (cost) for other routing protocols.
- If you want to redistribute non-RIP routes, select *Connected*, *Static*, or *RIP* and then enter the metric to use.
- If you want to change the default timer values, enter the number of seconds in the *Update*, *Timeout*, and *Garbage* fields.

- Go to *Router > Config > Access Lists* and select *Add Access List*.

Add Access List

ID ?
This value is required.

Strategy Prefix

Comments

Cancel Add

- Enter an identifier with all digits (in the range of 1-99).
- Enter an optional description of the access list.
- Select *Add*.
- Select *Config Rules* in the row for the access list that you just created.

Config Access List Rules

ID 56

Strategy Wildcard

Comments

Rules

ID(1-65535)	Action	Wildcard	Manage

+ Add Rule

Cancel Update

- Select *Add Rule*.
- Enter an identifier (1-65535), select *Deny* or *Permit* to specify if the rule will block or allow the specified IP addresses, and enter the Cisco-style wildcard filter.
- Select *Add Rule* if you want to add more rules.
- After you have added all of the rules that you want in the access list, select *Update* to save the rules you added.

- Go to *Router > Config > RIP > Distances* and select *Add RIP Distance*.

Add RIP Distance

Distance ID	<input type="text"/>	(0-4294967295)
	This value is required.	
Distance	<input type="text"/>	(1-255)
	This value is required.	
Access List	<input type="text" value="None"/>	
IP/Netmask	<input type="text" value="0.0.0.0/0.0.0.0"/>	
	<input type="button" value="Cancel"/>	<input type="button" value="Add"/>

- Enter the distance identifier in the Distance ID field.
 - Enter the distance.
 - Select the access list that you added in the previous step.
 - Enter the IP address and netmask, separated with a space or with a slash. For example, enter 1.2.3.4/5 or 1.2.3.4 248.0.0.0.
 - Select *Add*.
- Go to *Router > Config > RIP > Networks* and select *Add Network*.

Add RIP Network

Network ID	<input type="text"/>	(1-2147483647)
	This value is required.	
IP/Netmask	<input type="text"/>	
	This value is required.	
	<input type="button" value="Cancel"/>	<input type="button" value="Add"/>

- Enter an IP address and netmask for your RIP network, separated with a slash, and select *Add*. For example, enter 172.168.200.0/255.255.255.0. **NOTE:** Select an IP address for a network that includes all SVIs that you want to use. You can configure multiple network ranges to cover all SVIs that will be using RIP routing.

- Go to *Router > Config > RIP > Interfaces* and select *Configure RIP* for the appropriate interface.

Add RIP Interface

Interface	internal
Send Version	Global ▼
Receive Version	Global ▼
Passive Interface	<input type="checkbox"/>

Authentication

Authentication	<input checked="" type="radio"/> None <input type="radio"/> Text <input type="radio"/> MD5
----------------	--

- If you want to change the RIP version used to send and receive routing updates, select from the *Send Version* and *Receive Version* drop-down menus.
- If you do not want to send RIP updates from this interface, select *Passive Interface*.
- If you want to use authentication, select *Text* or *MD5*.
- Select *Add*.

Using the CLI:

```

config router rip
  config network
    edit <network identifier>
      set prefix <network prefix> <mask>
    next
  end
end

```

Checking the RIP configuration

The `get router info rip` command has options to display different aspects of the RIP configuration and status. For example, there are options to display the RIP general information and the RIP database:

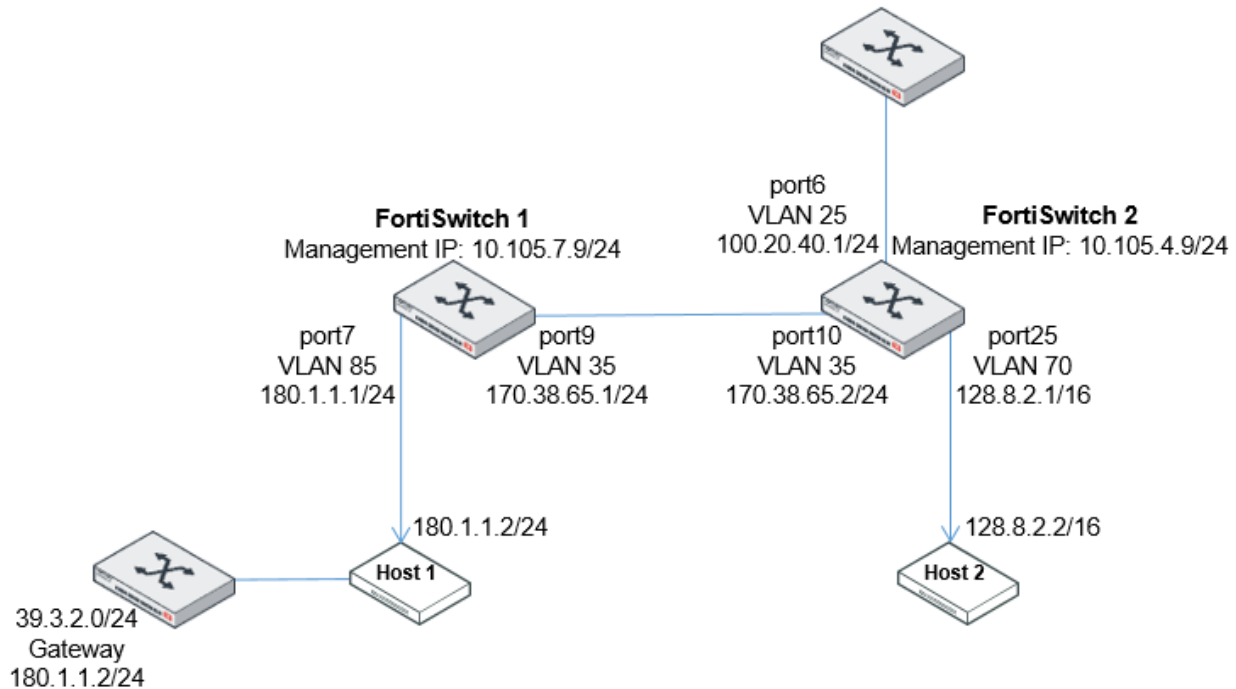
```

get router info rip status
get router info rip database

```

Example configuration

The following example shows a very simple RIP network:



Switch 1: Configure the switch interface

```
config switch interface
  edit "port9"
    set allowed-vlans 35
  next
  edit "port7"
    set allowed-vlans 85
  next
end
```

Switch 1: Configure the system interface

```
config system interface
  edit "vlan35"
    set ip 170.38.65.1/24
    set allowaccess ping https http ssh snmp telnet
    set vlanid 35
  next
  edit "vlan85"
    set ip 180.1.1.1/24
    set allowaccess ping https http ssh snmp telnet
    set vlanid 85
  next
end
```

Switch 1: Configure the RIP router; add authentication between FortiSwitch 1 and FortiSwitch 2

```
config router rip
  config network
    edit 1
      set prefix 170.38.65.0/24
    next
    edit 2
      set prefix 180.1.1.0/24
    next
  end
  config interface
    edit "vlan35"
      set auth-mode text
      set auth-string simplepw1
    next
  end
end
```

Switch 1: Add a static route and redistribute it

```
config router static
  edit 1
    set dst 39.3.2.0 255.255.255.0
    set gateway 180.1.1.2
    set status enable
  next
end

config router rip
  config redistribute "static"
    set status enable
  next
end
```

Switch 2: Configure the switch interface

```
config switch interface
  edit "port10"
    set allowed-vlans 35
  next
  edit "port25"
    set allowed-vlans 70
  next
end
```

Switch 2: Configure the system interface

```
config system interface
  edit "vlan35"
    set ip 170.38.65.2/24
    set allowaccess ping https http ssh snmp telnet
    set vlanid 35
  next
  edit "vlan70"
    set ip 128.8.2.1/16
```

```
        set allowaccess ping https http ssh snmp telnet
        set vlanid 70
    next
end
```

Switch 2: Configure the RIP router; add authentication between FortiSwitch 1 and FortiSwitch 2

```
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
```

Switch 2: Add a connected route and redistribute it

```
config switch interface
    edit "port6"
        set allowed-vlans 25
    next
end
config system interface
    edit "vlan25"
        set ip 100.20.40.1/24
        set allowaccess ping https http ssh snmp telnet
        set vlanid 25
    next
end

config router rip
    config redistribute "connected"
        set status enable
    next
end
```

VRRP

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

The Virtual Router Redundancy Protocol (VRRP) uses virtual routers to control which physical routers are assigned to an access network. A VRRP group consists of a master router and one or more backup routers that share a virtual IP address. If the master router fails, the VRRP automatically assigns one of the backup routers without affecting network traffic. When the failed router is functioning again, it becomes the master router again. VRRP provides this redundancy without user intervention or additional configuration to any of the devices on the network.

To create a VRRP group, you need to create a VRRP virtual MAC address, which is a shared MAC address adopted by the VRRP master. The VRRP virtual MAC address feature is disabled by default. You must enable the VRRP virtual MAC address feature on all members of a VRRP group.

The VRRP master router sends VRRP advertisement messages to the backup routers. When the VRRP master router fails to send advertisement messages, the backup router with the highest priority takes over as the master router.

For additional information about VRRP, see the [VRRP section of the FortiOS Handbook](#).

This chapter covers the following topics:

- [Configuring VRRP on page 224](#)
- [Checking the VRRP configuration on page 225](#)

Configuring VRRP

Using the GUI:

1. Go to *System > Network > Interface > Physical*.
2. Select *Edit* for the appropriate interface.
3. Select *Add VRRP* to add a virtual router.
 - Enter the unique virtual router identifier.
 - Enter the VRRP group number.
 - Enter the priority. If the highest priority value of 255 is entered, the virtual router becomes the master router.
 - Select *Preempt* if you want the router to preempt the master virtual router if the priority changes.
 - Enter the source virtual IP address that will be shared across the VRRP group.
 - Enter one or two IP addresses that the master router must track. The maximum number of IP addresses is two. If these IP addresses cannot be reached by the master router, the priority of the master router changes to 0.
 - Select *Add VRRP* to add each additional virtual router.
4. After filling in the fields for the virtual routers, select *Update*.

Using the CLI:

```
config system interface
  edit <VLAN name>
    set ip <IP address> <netmask>
    set allowaccess <access_types>
    set vrrp-virtual-mac enable
    config vrrp
      edit <VRRP router identifier>
        set priority <priority number>
        set vrgrp <VRRP group number>
        set vrip <virtual IP address>
      next
    end
    set snmp-index <index number>
    set vlanid <VLAN identifier>
    set interface "internal"
  next
end
```

Example of configuring 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
```

Checking the VRRP configuration

Use the `get router info vrrp` command to display the VRRP status:

```
get router info vrrp
```

BGP routing

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

Border Gateway Protocol (BGP) is an inter Autonomous System (AS) routing protocol. It is the main protocol to connect ISP networks across the world.

The current version of BGP is version 4 and defined in RFC- 4271. BGP uses TCP for transport protocol.

BGP is a path-vector protocol. It makes routing decision based on path and network policies rather than hop-count metric (RIP) or cost-factor metrics (OSPF).

You must explicitly configure peers to exchange routing information. There is no discovery in BGP.

FortiSwitchOS supports BGP-4 as described in RFC 4271.

This chapter covers the following topics:

- [Terminology on page 226](#)
- [Configuring BGP on page 226](#)
- [Sample configurations on page 228](#)

Terminology

An autonomous system (AS) is a group of one or more routers run by a network operator or service provider which has a single and clearly defined routing policy and is under single administration. Usually, the network operator will run an internal gateway protocol (such as OSPF, IS- etc) within the AS, and use BGP between AS's.

Each AS has a number that acts as a unique international identifier. AS numbers can be purchased from IANA.

External BGP (EBGP) is a variation of BGP which involves packet crossing multiple ASs. Confederation uses EBGP.

Internal BGP (IBGP) involves routing packets within a single AS. Router reflector uses iBGP. Routes learned using IBGP have a higher priority than the routes learned using EBGP.

BGP speaker router is a router that advertises routes to its peers using configured policies.

The FortiSwitch unit connects to neighbors as a BGP peer. The FortiSwitch unit is a BGP speaker node and advertise its routes. The FortiSwitch unit accepts routes with BGP and adds these routes to its local routing tables.

Configuring BGP

Configuring BGP on the FortiSwitch unit includes the following major steps:

1. Enter the BGP configuration mode.
2. Set the autonomous system and router identifier.
3. Configure a BGP neighbor.
4. Redistribute non-BGP routes. Advertise these non-BGP routes within BGP.

1. Enter the BGP configuration mode

Enter the BGP configuration mode to access all of the BGP configuration command:

```
# config router bgp
```

2. Set the autonomous system and router identifier

Set the autonomous system. For IBGP, the AS value needs to match the `remote-as` value in the neighbor router. For EBGP, the AS value differs from the `remote-as` value in the neighbor router. You also need to specify a fixed router identifier for the FortiSwitch unit. These two commands are mandatory.

```
# set as <AS number>
# set router-id <IP_address>
```

3. Configure the BGP neighbors

Configure the BGP neighbors.

NOTE: For IBGP, if the IP address of the BGP neighbor is a loopback address, you must use the `set update-source` cmd command to specify which interface address will be used as the source IP address in the outgoing BGP packet.

```
config neighbor
  edit <IP address>
    set remote-as <1-4294967295>
  end
```

4. Redistribute non-BGP routers

Redistribute non-BGP routes within BGP:

```
config redistribute {connected | isis | ospf | rip | static}
  set status enable
  set route-map <string>
end
```

Other BGP commands

Clearing the BGP routes

Use the following commands to clear the BGP routes:

```
execute router clear bgp all
execute router clear bgp ip <IP address>
execute router clear bgp as <AS_number>
execute router clear bgp dampening <IP_address>
```

Checking the BGP configuration

The `get router info bgp` command has options to display different aspects of the BGP configuration and status.

For example:

```
get router info bgp neighbors
get router info bgp network
```

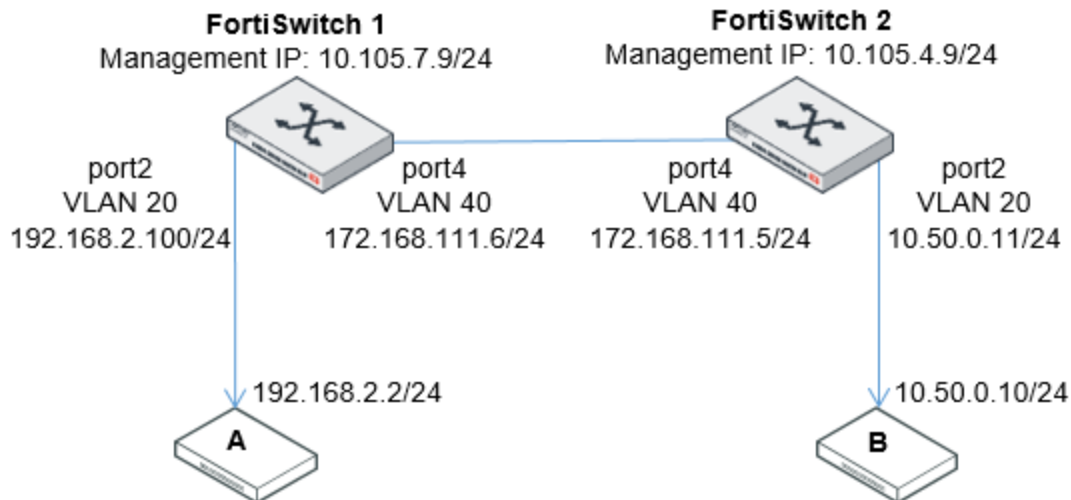
Changing the maximum number of paths for ECMP

If you are using equal-cost multi-path (ECMP) routing with the EBGP or IBGP, the maximum number of paths is 1 by default. Use the following commands to change the default:

```
config router bgp
  set maximum-paths-ebgp <1-64>
  set maximum-paths-ibgp <1-64>
end
```

Sample configurations

Here is an example of a BGP routing configuration:



Configure system interfaces

Interface configuration for FortiSwitch 1:

```
config system interface
  edit mgmt
    set ip 10.105.7.9 255.255.255.0
    set allowaccess ping https http ssh telnet
    set type physical
  next
  edit internal
    set type physical
  next
  edit vlan20-p2
    set ip 192.168.2.100 255.255.255.0
    set allowaccess ping https http ssh telnet
    set vlanid 20
    set interface internal
```

```
next
edit vlan40-p4
  set ip 172.168.111.6 255.255.255.0
  set allowaccess ping https http ssh telnet
  set vlanid 40
  set interface internal
end
config switch interface
edit "port2"
  set native-vlan 20
  set stp-state disabled
next
edit "port4"
  set native-vlan 40
  set stp-state disabled
next
edit "internal"
  set allowed-vlans 1,20, 40, 4094
  set stp-state disabled
next
end
```

Internal BGP

In this example, the two neighboring switches are in the same autonomous system.

Configuration for FortiSwitch 1:

```
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
```

Configuration for FortiSwitch 2:

```
config router bgp
  set as 6500
  set router-id 5.6.7.8
  config neighbor
    edit "172.168.111.6"
      set remote-as 6500
    next
  end
  config network
    edit 1
```

```
        set prefix 10.50.2.0 255.255.255.0
    next
end
    config redistribute "connected"
end
end
end
```

External BGP

In this example, the two neighboring switches are in separate autonomous systems.

Configuration for FortiSwitch 1:

```
config router bgp
    set as 6500
    set router-id 1.2.3.4
    config neighbor
        edit "172.168.111.5"
            set remote-as 7500
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
    config redistribute "connected"
end
end
```

Configuration for FortiSwitch 2:

```
config router bgp
    set as 7500
    set router-id 5.6.7.8
    config neighbor
        edit "172.168.111.6"
            set remote-as 6500
        next
    end
    config network
        edit 1
            set prefix 10.50.2.0 255.255.255.0
        next
    end
    config redistribute "connected"
end
end
```

Using the following command, you can check the BGP status on the local switch:

```
# get router info bgp summary
```

To check the details about the BGP neighbors:

```
# get router info bgp neighbors
```

To check the routes learned by BGP, use the following command:

```
# get router info routing-table details
```

PIM routing

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

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.

NOTE:

- Access lists, prefix lists, and route maps are not supported.
- Bidirectional forwarding detection (BFD) is not supported.
- You cannot use PIM and the IGMP querier at the same time on the same switched virtual interface.
- PIM and IGMP snooping work independently.
- IPv6 is not supported.
- IGMP version-3 explicit membership tracking is not supported.
- SSM mapping is not supported.
- The multicast routing information base (MRIB) is not supported.
- The PIM management information base (MIB) is not supported.

This chapter covers the following topics:

- [Terminology on page 232](#)
- [Configuring PIM on page 232](#)
- [Checking the PIM configuration on page 233](#)

Terminology

PIM domain: A PIM domain is a logical area comprising a number of contiguous networks. The domain contains at least one Boot Strap Router (BSR) and a number of Rendezvous Points (RPs) and Designated Routers (DRs).

RP: An RP represents the root of a non-source-specific distribution tree to a multicast group.

Configuring PIM

To configure a PIM domain:

1. Determine the appropriate paths for multicast packets.
2. Make a note of the interfaces that will be PIM enabled. These interfaces can run a unicast routing protocol.
3. If you want multicast packets to be handled by specific (static) rendezvous points (RPs), record the IP addresses of the PIM-enabled interfaces on those RPs.

4. Enable PIM version 4 on all participating routers between the source and receivers. Use the `config router multicast` command to set global operating parameters.
5. Configure the PIM routers that have good connections throughout the PIM domain to be candidate boot strap routers (BSRs).
6. Configure one or more of the PIM routers to be candidate RPs.
7. If required, adjust the default settings of PIM-enabled interface(s).

To configure the source allowed for a multicast flow:

```
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 source-addr <IP_address>
      end
    end
  end
```

To configure a FortiSwitch unit to support PIM:

```
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>
      set dr-priority <1-4294967295>
      set multicast-flow <string>
      config igmp
        set query-interval <1-65535>
        set query-max-response-time <1-25>
      end
    end
  end
```

Checking the PIM configuration

Use the following commands to check your PIM configuration:

```
get router info multicast config
get router info multicast igmp {groups | sources | querier | interface | join |
  parameters}
get router info multicast pim {neighbour | interface}
```

IS-IS routing

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

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).

IS-IS is a link state protocol that is well-suited to smaller networks. It is in widespread use and has near universal support on routing hardware. It is quick to configure and works well if there are no redundant paths. However, IS-IS updates are sent out node-by-node, so it can be slow to find a path around network outages. IS-IS also lacks good authentication, can not choose routes based on different quality-of-service methods, and can create network loops if you are not careful. IS-IS uses Dijkstra's algorithm to find the best path, like OSPF.

While OSPF is more widely known, IS-IS is a viable alternative to OSPF in enterprise networks and ISP infrastructures, largely due to its native support for IPv6 and its nondisruptive methods for splitting, merging, migrating, and renumbering network areas.

This chapter covers the following topics:

- [Terminology on page 234](#)
- [Configuring IS-IS on page 234](#)
- [Checking the IS-IS configuration on page 235](#)

Terminology

TLV: IS-IS uses type-length-value (TLV) parameters to carry information in Link-State PDUs (LSPs). The TLV field consists of one octet of type (T), one octet of length (L), and "L" octets of value (V).

Link-state PDU (LSP): The LSP contains information about each router in an area and its connected interfaces.

Complete sequence number PDU (CSNP): CSNPs contain a list of all LSPs in the current LSDB.

Authentication keychain: A keychain is a list of one or more authentication keys including the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes.

Configuring IS-IS

The following is an example of an IS-IS configuration:

```
config router isis
  set default-information-metric 60
  config isis-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 isis-net
    edit 1 set net 1.0000.0000.0000.2.00
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
```

Configuring BFD for IS-IS

You can use bidirectional forwarding detection (BFD) for the IS-IS routing protocol:

```
config router isis
    config isis-interface
        edit <IS-IS interface name>
            set bfd {enable| disable}
        next
    end
end
```

For example, if you want to enable BFD on vlan100:

```
config router isis
    config isis-interface
        edit "vlan100"
            set bfd enable
        next
    end
end
```

Checking the IS-IS configuration

Use the following commands to check your IS-IS configuration:

```
get router info isis interface
get router info isis route
get router info isis summary
get router info isis topology
```

Users and user groups

The FortiSwitch unit provides authentication mechanisms to control user access to the system (based on the user group associated with the user). The members of user groups are user accounts. Local users and peer users are defined on the FortiSwitch unit. User accounts can also be defined on remote authentication servers.

This section describes how to configure local users and peer users and how to configure user groups. For information about configuring the authentication servers, see [Remote authentication servers on page 36](#).

This chapter covers the following topics:

- [Users on page 236](#)
- [User groups on page 237](#)

Users

A user account consists of a user name, password, and potentially other information, configured in a local user database or on an external authentication server.

Users can access resources that require authentication only if they are members of an allowed user group.

Using the GUI:

1. Go to *System > User > Definition*.
2. Select *Add User*.
3. Enter the user name.
4. Select *Enable* to make the user account active.
5. Enter the password for the user account. Passwords can be up to 64 characters in length.
6. Select *Add*.

Using the CLI:

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

Field	Description
user_name	Identifies the user

Field	Description
password_string	A password for the local user. Passwords can be up to 64 characters in length.
ldap-server <server_name>	To authenticate this user using a password stored on a remote authentication server, select the type of server and then select the server from the list. You can select only a server that has already been added to the FortiSwitch configuration.
radius-server <server_name>	
tacacs+-server <server_name>	
status	Enable or disable this user.

User groups

A user group contains a list of local and remote users.

Security policies allow access to specified user groups only. This restricted access enforces Role Based Access Control (RBAC) to your organization's network and its resources. Users must be in a group and that group must be part of the security policy.

Using the GUI:

1. Go to *System > User > Group*.
2. Select *Add Group*.
3. Enter the group name.
4. Select which available users will be members of the new user group.
5. *Enable* to make the user account active.
6. If you want to use an authentication server, select *Add Server*.
 - Select the server name. If no server name is available, go to *System > Authentication* to add an authentication server.
 - Enter a group name or select *Any*.
7. Select *Add Group*.

Using the CLI:

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

The following table describes the parameters:

Field	Description
groupname	Identifies the user group.
authtimeout <timeout>	Sets the authentication timeout for the user group. The range is 1 to 480 minutes. If this field is set to 0, the global authentication timeout value is used.
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"> • <code>firewall</code>—FortiSwitch users defined in user local, user ldap, or user radius • <code>fssso-service</code>—Directory Service users
http-digest-realm <attribute>	Enter the realm attribute for MD5-digest authentication.
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.
config match fields	
<match_id>	Enter an ID for the entry.
group-name <gname_str>	Identifies the matching group on the remote authentication server.
server-name <srvname_str>	Specifies the remote authentication server.

802.1x authentication

To control network access, the FortiSwitch unit supports IEEE 802.1x authentication. A supplicant connected to a port on the switch must be authenticated by a RADIUS/Diameter server to gain access to the network. The supplicant and the authentication server communicate using the switch using EAP. The FortiSwitch unit supports EAP-PEAP, EAP-TTLS, EAP-TLS, and EAP-MD5.

To use the RADIUS server for authentication, you must configure the server before configuring the users or user groups on the FortiSwitch unit.

The FortiSwitch unit implements MAC-based authentication. The switch saves the MAC address of each supplicant's device. The switch provides network access only to devices that have successfully been authenticated.

The FortiSwitch unit supports up to 20 devices per port for 802.1x MAC-based authentication. System-wide, the FortiSwitch unit now supports a total of 10 times the number of interfaces for 802.1x MAC-based authentication:

Model	Total number of devices supported per switch
108	80
112	120
124/224/424/524/1024	240
148/248/448/548/1048	480
3032	320

You can enable the MAC Authentication Bypass (MAB) option for devices (such as network printers) that cannot respond to the 802.1x authentication request. With MAB enabled on the port, the system will use the device MAC address as the user name and password for authentication.

Optionally, you can configure a guest VLAN for unauthorized users. Alternatively, you can specify a VLAN for users whose authentication was unsuccessful.

When you are testing your system configuration for 802.1x authentication, you can use the monitor mode to allow network traffic to flow, even if there are configuration problems or authentication failures.

This chapter covers the following topics:

- [Dynamic VLAN assignment on page 240](#)
- [MAC authentication bypass \(MAB\) on page 241](#)
- [Configuring global settings on page 243](#)
- [Configuring the 802.1x settings on an interface on page 245](#)
- [Viewing the 802.1x details on page 249](#)
- [Using the monitor mode on page 251](#)
- [Clearing port authorizations on page 251](#)
- [Authenticating users with a RADIUS server on page 252](#)
- [Authenticating an admin user with RADIUS on page 258](#)
- [RADIUS accounting and FortiGate RADIUS single sign-on on page 261](#)
- [RADIUS change of authorization \(CoA\) on page 263](#)

- Use cases on page 266
- Detailed deployment notes on page 269

Dynamic VLAN assignment

You can configure the RADIUS server to return a VLAN in the authentication reply message.

1. On the FortiSwitch unit, select port-based authentication or MAC-based authentication and a security group.
2. On the RADIUS server, configure the attributes.

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select a port and then select *Edit*.

Physical Port Interfaces

Name	Traffic (Last Day)	Native / Allowed VLANs	Security Mode	STP	Edge Port	Loop Guard	sFlow
internal		4094 / 1,4094	None	-	✓	-	-
port1		1	None	✓	✓	-	-
port3		1	802.1X MAC-Based	✓	✓	-	-
port4		1	802.1X	✓	✓	-	-

3. Select *802.1X* for port-based authentication or select *802.1X-MAC-based* for MAC-based authentication.

Port Security

- Security Mode**
- None
 - 802.1X
 - 802.1X-MAC-based

4. Select one or more security groups.
5. Select *OK*.

Using the CLI:

To select port-based authentication and the security group on the FortiSwitch unit:

```
config switch interface
  edit <interface_name>
    config port-security
      set port-security-mode 802.1X
    end
    set security-groups <security-group-name>
  end
```

The FortiSwitch unit will change the native VLAN of the port to that of the VLAN from the server.

To select MAC-based authentication and the security group on the FortiSwitch unit:

```
config switch interface
  edit <interface_name>
    config port-security
      set port-security-mode 802.1X-mac-based
    end
    set security-groups <security-group-name>
  end
```

Here, the switch assigns the returned VLAN only to this user's MAC address. The native VLAN of the port remains unchanged.

Use the following configuration command to view the MAC-based VLAN assignments:

```
diagnose switch vlan assignment mac list [sorted-by-mac | sorted-by-vlan]
```

Configure the following attributes in the RADIUS server:

- Tunnel-Private-Group-Id—VLAN ID or name (10)
- Tunnel-Medium-Type—IEEE-802 (6)
- Tunnel-Type—VLAN (13)

NOTE: If the Tunnel-Private-Group-Id attribute is set to the VLAN name, the same string must be specified in the `set description` command under the `config switch vlan` command. For example:

```
config switch vlan
  edit 100
    set description "local_vlan"
  next
end
```

MAC authentication bypass (MAB)

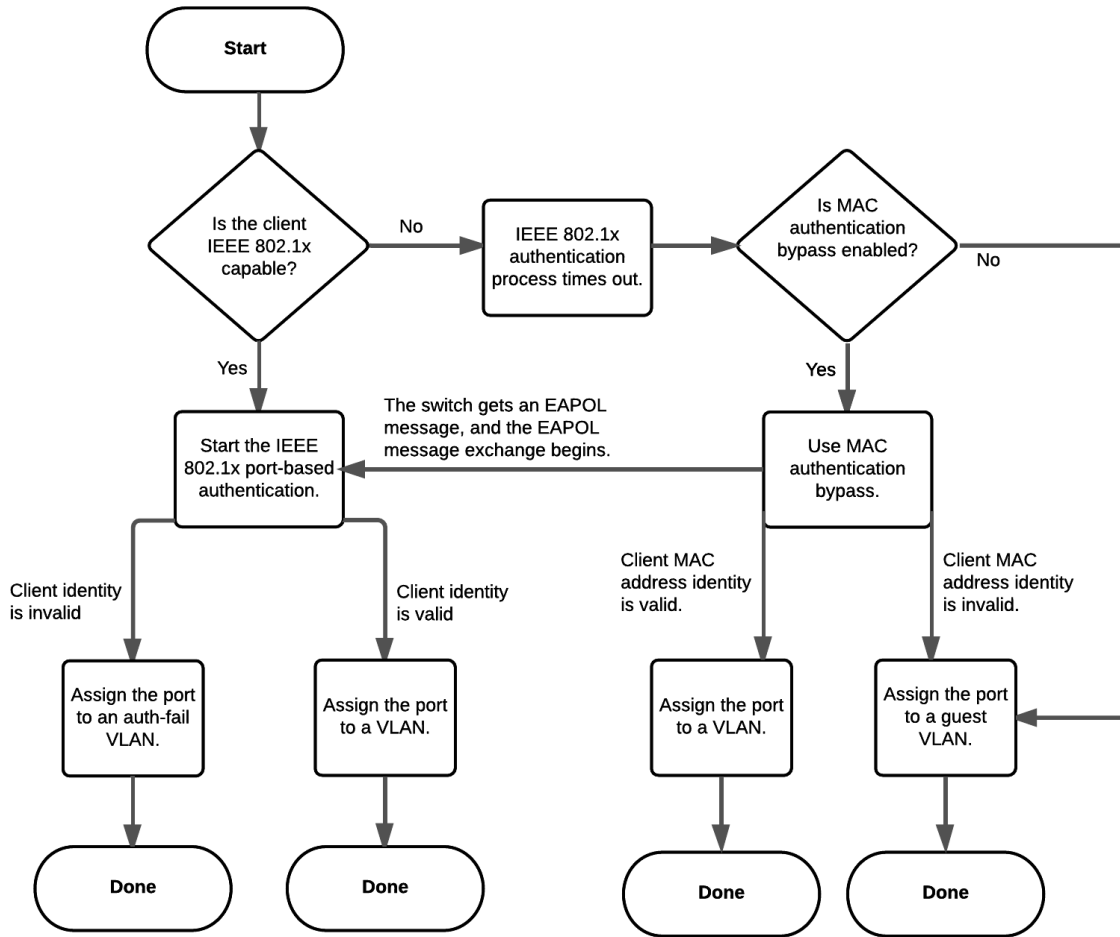
Devices such as network printers, cameras, and sensors might not support 802.1x authentication. If you enable the MAB option on the port, the system will use the device MAC address as the user name and password for authentication.

MAB retries authentication three times before the device is assigned to a guest VLAN for unauthorized users. By default, reauthentication is disabled. Use the following commands if you want to change the default behavior:

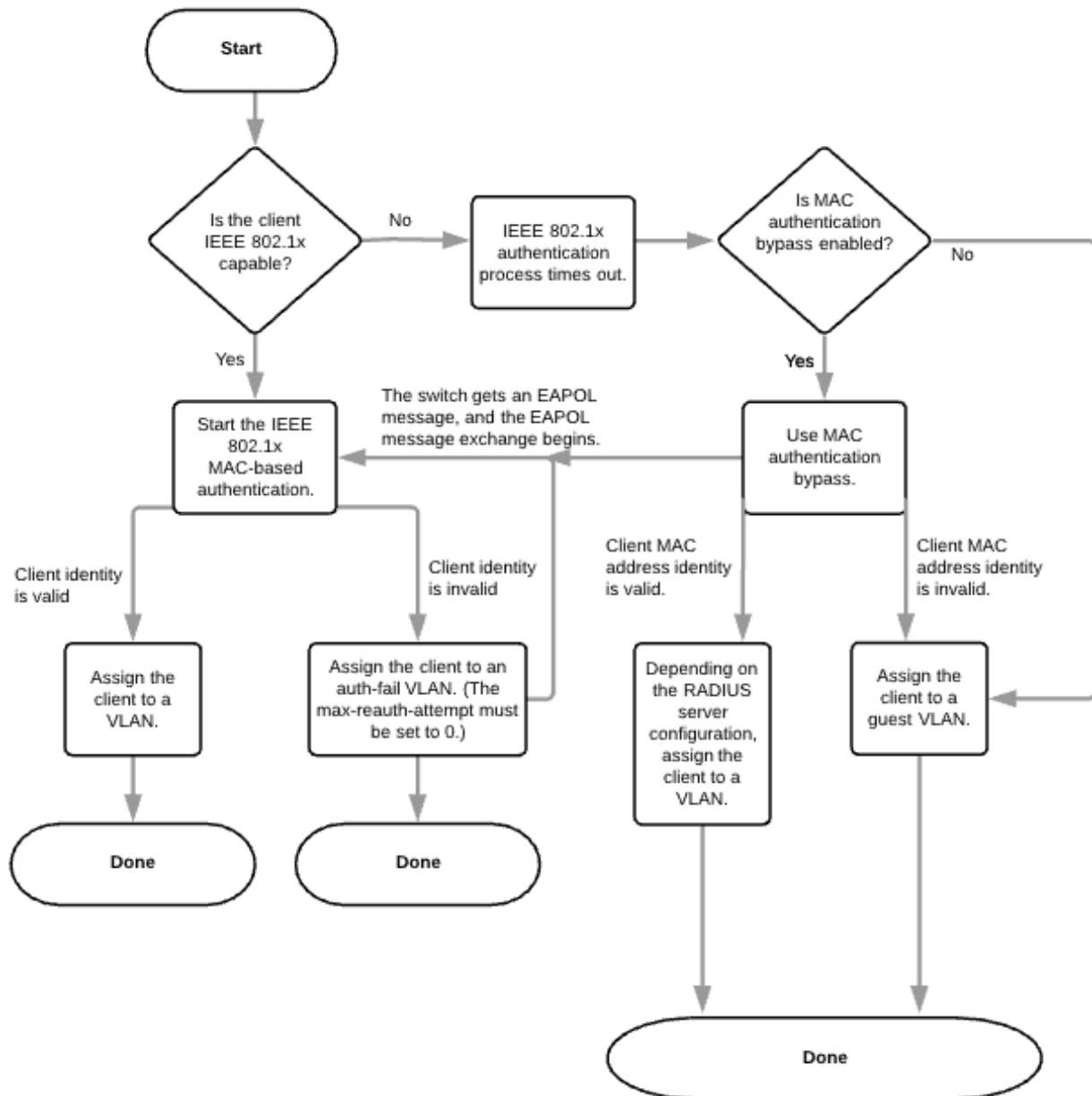
```
config switch global
  config port-security
    set mab-reauth enable
  end
```

You must provision the RADIUS server to authenticate the devices that use MAB, either by adding the MAC addresses as regular users or by implementing additional logic to resolve the MAC addresses in a network inventory database.

The following flowchart shows the FortiSwitch 802.1x port-based authentication with MAB enabled:



The following flowchart shows the FortiSwitch 802.1x MAC-based authentication with MAB enabled:



Configuring global settings

To select which 802.1x certificate and certificate authority that the FortiSwitch unit uses, see [SSL configuration on page 55](#).

Using the GUI:

1. Go to *Switch > Interface > Port Security*.

Port Security Settings

Link Down Behavior

- Require Reauthentication
 Do Not Require Reauthentication

802.1x/MAB

- Reauthorization Period Minutes (1-1440)
- Reauthorization Attempts Maximum (1-15)

Update

2. Select *Reauthorization Period* and then enter the number of minutes before the system requires the device to reauthenticate.
3. Select *Reauthorization Attempts* and then enter the maximum number of times that the system will try to reauthorize the session.
4. Select *Require Reauthentication* to revert all devices to the unauthenticated state if the link goes down or select *Do Not Require Reauthentication* if reauthentication is unnecessary if the link goes down.
5. Select *Update*.

Using the CLI:

```

config switch global
  config port-security
    set link-down-auth {no-action | set-unauth}
    set mab-reauth {enable | disable}
    set max-reauth-attempt <0-15>
    set quarantine-vlan {enable | disable}
    set reauth-period <0-1440>
  end
  
```

NOTE: Changes to global settings only take effect when new 802.1x/MAB sessions are created.

Variable	Description
link-down-auth	If a link goes down, this setting determines whether the impacted devices must reauthenticate. Set the value to <code>no-action</code> if reauthentication is unnecessary. Set the value to <code>set-unauth</code> to revert all devices to the unauthenticated state. Each device must reauthenticate. The default is <code>set-unauth</code> .
mab-reauth	Enable or disable whether MAB retries authentication before assigning a device to a guest VLAN for unauthorized users. By default, this option is disabled.
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. The default value is 3.

Variable	Description
quarantine-vlan	Enable or disable quarantine VLAN detection. Enable this setting to use quarantines with 802.1x MAC-based authentication in FortiLink mode. By default, this option is enabled.
reauth-period	This setting defines how often the device needs to reauthenticate (that is, if a session remains active beyond this number of minutes, the system requires the device to reauthenticate). The default value is 60 minutes. Set the value to 0 to disable reauthentication.

Configuring the 802.1x settings on an interface

Using the GUI:

1. Go to *Switch > Interface > Physical*.

2. Select a port and then select *Edit*.

Edit Physical Port Interface

Name	port1	
Private VLAN	<input checked="" type="radio"/> Disable <input type="radio"/> Promiscuous <small>+</small> <input type="radio"/> Sub-VLAN <small>+</small>	
Native VLAN	<input type="text" value="1"/>	(1-4095)
Allowed VLANs	<input type="text"/>	(1-4095)
Enable STP	<input type="checkbox"/>	
Enable Edge Port	<input type="checkbox"/>	
Enable sFlow	<input type="checkbox"/>	
Enable Loop Guard	<input type="checkbox"/>	

DHCP Snooping

DHCP Snooping	<input checked="" type="radio"/> Untrusted <input type="radio"/> Trusted	
Option 82 Trust	<input type="checkbox"/>	

IGMP Snooping

IGMP Snooping	<input type="checkbox"/>	
Flood Reports	<input type="checkbox"/>	
Flood Traffic	<input type="checkbox"/>	

QoS Policy

QoS Policy	<input type="text" value="default"/>	
Trust 802.1p	<input type="text" value="None"/>	
Trust IP-DSCP	<input type="text" value="None"/>	

Port Security

Security Mode	<input checked="" type="radio"/> None <input type="radio"/> 802.1X <input type="radio"/> 802.1X-MAC-Based	
---------------	---	--

3. Select *802.1X* for port-based authentication or select *802.1X-MAC-based* for MAC-based authentication. The Port Security section displays additional options.

Port Security

Security Mode	<input type="radio"/> None <input checked="" type="radio"/> 802.1X <input type="radio"/> 802.1X MAC-Based
MAC Auth Bypass	<input type="checkbox"/>
EAP Pass-Through Mode	<input type="checkbox"/>
Frame VLAN Apply	<input checked="" type="checkbox"/>
Open Authentication	<input type="checkbox"/>
Guest VLAN	<input type="checkbox"/>
Guest VLAN ID	<input type="text" value="100"/> (1-4095)
Guest Auth Delay	<input type="text" value="5"/> (1-900)
Auth Fail VLAN	<input type="checkbox"/>
Auth Fail VLAN ID	<input type="text" value="200"/> (1-4095)
RADIUS Session Timeout	<input type="checkbox"/>
Security Groups (Select At Least One)	<input type="checkbox"/> NewRADIUSgroup <input type="checkbox"/> RADIUS_Admins <input type="checkbox"/> Radius_group This value is required.

Cancel OK

- Select one or more security groups.
- Select *MAC Auth Bypass*.
- Select *EAP Pass-Through Mode*.

NOTE: *EAP Pass-Through Mode* is enabled by default, which is the recommended setting. If the RADIUS authentication server does not support EAP-TLS, the *EAP Pass-Through Mode* needs to be disabled.
- Select *Frame VLAN Apply*.
- Select *Open Authentication*.
- Select *Guest VLAN* if you want to assign a VLAN to unauthorized users. If you select *Guest VLAN*, enter the guest VLAN identifier in the *Guest VLAN ID* field.
- In the *Guest Auth Delay* field, enter the number of seconds for an unauthorized user to have access as a guest before authorization fails.
- Select *Auth Fail VLAN* if you want to assign a VLAN to users who attempted to authenticate but failed to provide valid credentials. If you select *Auth Fail VLAN*, enter the VLAN identifier in the *Auth Fail VLAN ID* field.
- If you want to use the RADIUS-provided reauthentication time, select *RADUS Session Timeout*.
- Select **OK**.

Using the CLI:

```
config switch interface
edit <port>
```

```

config port-security
  set mab-eapol-request <0-10>
  set port-security-mode {none | 802.1X | 802.1X-mac-based}
  set framevid-apply {disable | enable}
  set auth-fail-vlan {enable | disable}
  set auth-fail-vlanid <vlanid>
  set eap-passthru {enable | disable}
  set guest-auth-delay <integer>
  set guest-vlan {enable | disable}
  set guest-vlanid <vlanid>
  set mac-auth-bypass {enable | disable}
  set open-auth {enable | disable}
  set radius-timeout-overwrite {enable | disable}
end
set security-groups <security-group-name>
end

```

Variable	Description	Default
mab-eapol-request <0-10>	<p>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.</p> <p>To disable this feature, set <code>mab-eapol-request</code> to 0 or disable <code>macauth-bypass</code>.</p>	3
port-security-mode {none 802.1X 802.1X-mac-based}	<p>Set the security mode for the port. None (no security) is the default. Set the security mode to <code>802.1X</code> for port-based authentication or <code>802.1X-mac-based</code> for MAC-based authentication. If you change the security mode from none, you must set the security group with the <code>set security-groups</code> command.</p>	none
framevid-apply {disable enable}	<p>Enable or disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.</p> <p>NOTE: For phone and PC configuration only, disable <code>framevid-apply</code> to preserve the native VLAN when the data traffic is expected to be untagged.</p>	enable
auth-fail-vlan and guest-vlan	<p>The system assigns the <code>guest-vlan</code> to unauthorized users. After the system assigns the <code>auth-fail-vlan</code> to users who attempted to authenticate but failed to provide valid credentials.</p> <p>If you enable either <code>guest-vlan</code> or <code>auth-fail-vlan</code>, you must configure the corresponding VLAN ID (otherwise, the configuration save attempt will fail when you enter <code>next</code> or <code>end</code>).</p>	disable
eap-passthru {enable disable}	<p>Enable or disable the EAP pass-through mode.</p> <p>NOTE: EAP pass-through mode is enabled by default, which is the recommended setting. If the RADIUS authentication server does not support EAP-TLS, use <code>set eap-passthru disable</code> instead.</p>	enable

Variable	Description	Default
guest-auth-delay	Time in seconds when an authorization fails after the guest is applied.	5
mac-auth-bypass {enable disable}	Enable the feature. The default is disable.	disable
open-auth {enable disable}	Enable or disable open authentication (monitor mode) on this interface.	disable
radius-timeout-overwrite	<p>This setting specifies whether to use the RADIUS-provided re-authentication timeout. If the setting is enabled, the port uses the local timeout (see Configuring global settings on page 243).</p> <p>If the setting is disabled, the system uses the value of the RADIUS Access-Accept message Session-Timeout attribute to determine the duration of the session. It uses the Termination-Action value to determine the device action when the session's timer expires.</p> <p>If the Termination-Action attribute is present and its value is RADIUS-Request, the device port re-authenticates the host. If the Termination-Action attribute is not present, or its value is Default, the device port terminates the session.</p> <p>If the device port is configured to use the RADIUS-supplied timeout, but the Access-Accept message does not include a Session-Timeout attribute, the device port never re-authenticates the supplicant.</p>	disable
security-groups <security-group-name>	Enter the security group name if you are using port-based authentication or MAC-based authentication.	No default

Viewing the 802.1x details

Using the GUI:

Go to *Switch > Monitor > 802.1x Status*.

Using the CLI:

Use the following command to show diagnostics on one or all ports:

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

```
port3 : Mode: port-based (MAC by-pass disable)
      Link: Link up
```

```

Port State: authorized
Dynamic Authorized Vlan: 10
Native vlan: 10
Allowed vlan list: 1-10
Untagged vlan list:
Guest vlan:
AuthFail vlan:

Sessions info:
STA=00:24:9b:1b:20:65 Type=802.1X EAP PEAP state=AUTHENTICATED

```

```

port7 : Mode: mac-based (mac-by-pass disable)
Link: Link up
Port State: authorized ( )
EAP pass-through mode : Enable
Native Vlan : 1
Allowed Vlan list: 1
Untagged Vlan list: 1
Guest VLAN :

```

```

Client MAC Type Vlan Dynamic-Vlan
0a:0a:0b:0b:0a:0a 802.1x 1 0
0a:0a:0b:0b:0a:09 802.1x 1 0
0a:0a:0b:0b:0a:08 802.1x 1 0
0a:0a:0b:0b:0a:07 802.1x 1 0
0a:0a:0b:0b:0a:06 802.1x 1 0
0a:0a:0b:0b:0a:05 802.1x 1 0
0a:0a:0b:0b:0a:04 802.1x 1 0
0a:0a:0b:0b:0a:03 802.1x 1 0
0a:0a:0b:0b:0a:02 802.1x 1 0
0a:0a:0b:0b:0a:01 802.1x 1 0

```

```

Sessions info:
0a:0a:0b:0b:0a:0a Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3 param-
s:reAuth=3600
0a:0a:0b:0b:0a:09 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3
params:reAuth=3600
0a:0a:0b:0b:0a:08 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3 param-
s:reAuth=3600
0a:0a:0b:0b:0a:07 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3
params:reAuth=2896
0a:0a:0b:0b:0a:06 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3 param-
s:reAuth=3600
0a:0a:0b:0b:0a:05 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3
params:reAuth=3600
0a:0a:0b:0b:0a:04 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3 param-
s:reAuth=3600
0a:0a:0b:0b:0a:03 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3
params:reAuth=3600
0a:0a:0b:0b:0a:02 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3 param-
s:reAuth=3600
0a:0a:0b:0b:0a:01 Type=802.1x,MD5,state=AUTHENTICATED,etime=2,eap_cnt=3

```

```
params:reAuth=3600h=120
```

Using the monitor mode

Use the monitor mode to test your system configuration for 802.1x authentication. You can use monitor mode to test port-based authentication, MAC-based authentication, EAP pass-through mode, and MAC authentication bypass. After you enable monitor mode, the network traffic will continue to flow, even if the users fail authentication.

To enable monitor mode:

```
config switch interface
  edit <port_name>
    config port-security
      set port-security-mode {802.1X | 802.1X-mac-based}
      set open-auth enable
    end
  next
end
```

After `open-auth` mode is enabled, the port changes to an authorized monitor mode.

To confirm that the port is in monitor mode, use the `diagnose switch` command. For example:

```
S448DP3X15000009 # diag sw 8 status
port9 : Mode: port-based (mac-by-pass enable)
Link: Link up
Port State: authorized:open_auth ( )
Dynamic Authorized Vlan : 0
EAP pass-through mode : Enable
Native Vlan : 10
Allowed Vlan list: 10,20,30
Untagged Vlan list:
Guest VLAN :
Auth-Fail Vlan : 200

Sessions info:
00:09:0f:09:09:09      Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0
params:reAuth=3600"
```

Clearing port authorizations

Using the GUI:

1. Go to *Switch > Interface > Physical*.
2. Select one or more ports that you want to clear the authorization from.
3. Select *Clear Auth*.

Using the CLI:

```
execute 802-1x clear interface <port>
```

Authenticating users with a RADIUS server

Using the GUI:

1. Define the RADIUS server:
 - a. Go to *System > Authentication > RADIUS*.
 - b. Select *Add Server*.

Add RADIUS Server

Name	<input type="text"/>
Primary Server Address	<input type="text"/>
Primary Server Secret	<input type="text"/> <input type="button" value="📄"/>
Secondary Server Name/IP	<input type="text"/>
Secondary Server Secret	<input type="text"/> <input type="button" value="📄"/>
Authentication Scheme	<input checked="" type="radio"/> Use Default Authentication Scheme <input type="radio"/> Specify Authentication Protocol
NAS IP/Called Station ID	<input type="text"/>
Include in every User Group	<input type="checkbox"/>

- c. In the *Name* field, enter a name for the RADIUS server.
 - d. In the *Primary Server Address* field, enter the IP address for the RADIUS server.
 - e. In the *Primary Server Secret* field, enter a password to use as a RADIUS key.
 - f. Select *Add*.
2. Create a user group:
 - a. Go to *System > User > Group*.

- b. Select *Add Group*.

Add Group

Name

Members

Available Users



Members

Authentication Servers

[+ Add Server](#)

Name	Group Name	Manage
------	------------	--------

No servers specified

[Cancel](#) [Add Group](#)

- c. In the *Name* field, enter a name for the user group.
 - d. Select *Add Server*.
 - e. Select the name of the RADIUS server that you configured in step 1.
 - f. Select *Add Group*.
3. Configure the port security:
- a. Go to *Switch > Interface > Physical*.
 - b. Select a port and then select *Edit*.

Physical Port Interfaces

Name	Traffic (Last Day)	Native / Allowed VLANs	Security Mode	STP	Edge Port	Loop Guard	sFlow
Internal		4094 / 1, 4094	None	-	✓	-	-
port1		1	None	✓	✓	-	-
port3		1	802.1X MAC-Based	✓	✓	-	-
port4		1	802.1X	✓	✓	-	-

- c. Select *802.1X* for port-based authentication or select *802.1X-MAC-based* for MAC-based authentication.

Port Security

Security Mode

None

802.1X

802.1X-MAC-based

- d. Select the user group that you configured in step 2.

RADIUS Session Timeout

Security Groups (Select At Least One) NewRADIUSgroup
This value is required.

Cancel OK

- e. Select *OK*.

Using the CLI:

1. Define the RADIUS server:

```
config user radius
  edit <name>
    set server <address>
  end
end
```

2. Create a user group:

```
config user group
  edit <name>
    set member <list>
    config match
      edit 1
        set group-name <name>
        set server-name <name>
      end
    end
  end
end
```

3. Configure the switch interface for port-based 802.1x:

```
config switch interface
  edit <interface>
    config port-security
      set port-security-mode 802.1X
    end
    set security-groups <security-group-name>
  end
end
```

4. Configure the switch interface for MAC-based 802.1x:

```

config switch interface
  edit <interface>
    config port-security
      set port-security-mode 802.1X-mac-based
    end
    set security-groups <security-group-name>
  end
end

```



Example: RADIUS user group

Using the GUI:

1. Define the RADIUS server:

- a. Go to *System > Authentication > RADIUS*.
- b. Select *Add Server*.
- c. In the *Name* field, enter `FortiAuthenticator`.
- d. In the *Primary Server Address* field, enter `10.160.36.190`.
- e. In the *Primary Server Secret* field, enter
`6rF7O4/Zf3p2TutNyeSjPbQc73QrS21wNDmNXd/rg9k6nTR6yMhBRsJGpArhle6UOCb7b8InM3nr
CeuVETr/a02LpILmIltBq5sUMCNqbR6zp2fS3r35Eyd3IIRzmve4Vusi52c1MrCqVhzzy2EfxkBr
x5FhcRQWxStvnVt4+dzLYbHZ.`

Add RADIUS Server

Name	<input type="text" value="FortiAuthenticator"/>
Primary Server Address	<input type="text" value="10.160.36.190"/>
Primary Server Secret	<input type="password" value="....."/> 
Secondary Server Name/IP	<input type="text"/>
Secondary Server Secret	<input type="password"/> 
Authentication Scheme	<input checked="" type="radio"/> Use Default Authentication Scheme <input type="radio"/> Specify Authentication Protocol
NAS IP/Called Station ID	<input type="text"/>
Include in every User Group	<input type="checkbox"/>

- f. Select *Add*.

2. Create a user group:
 - a. Go to *System > User > Group*.
 - b. Select *Add Group*.
 - c. In the *Name* field, enter `Radius_group`.
 - d. Select *Add Server*.
 - e. Select *FortiAuthenticator* as the authentication server.

Add Group

Name

Members

Available Users

→

←

Members

Authentication Servers + Add Server

Name	Group Name	Manage
FortiAuthenticator ▾	<input checked="" type="radio"/> Any <input type="radio"/> Specify <input style="width: 100%;" type="text"/>	✖ Delete
Cancel Add Group		

- f. Select *Add Group*.
3. Configure the port security:
 - a. Go to *Switch > Interface > Physical*.
 - b. Select the *port1* row and then select *Edit*.

Physical Port Interfaces

Name	Traffic (Last Day)	Native / Allowed VLANs	Security Mode	STP	Edge Port	Loop Guard	sFlow
Internal		4094 / 1,4094	None	-	✓	-	-
port1		1	None	✓	✓	-	-
port3		1	802.1X MAC-Based	✓	✓	-	-
port4		1	802.1X	✓	✓	-	-

- c. In the *Allowed VLANs* field, enter 1.
 - d. Select *802.1X*.

e. Select *Radius_group*.

Edit Physical Port Interface

Name: port1

Private VLAN: Disable Promiscuous Sub-VLAN

Native VLAN: 1 (1-4095)

Allowed VLANs: 1 (1-4095)

Enable STP:

Enable Edge Port:

Enable sFlow:

Enable Loop Guard:

DHCP Snooping

DHCP Snooping: Untrusted Trusted

Option 82 Trust:

IGMP Snooping

IGMP Snooping:

Flood Reports:

Flood Traffic:

QoS Policy

QoS Policy: default

Trust 802.1p: None

Trust IP-DSCP: None

Port Security

Security Mode: None 802.1X 802.1X/MAC-Based

MAC Auth Bypass:

EAP Pass-Through Mode:

Frame VLAN Apply:

Open Authentication:

Guest VLAN:

Guest VLAN ID: 100 (1-4095)

Guest Auth Delay: 5 (1-900)

Auth Fail VLAN:

Auth Fail VLAN ID: 200 (1-4095)

RADIUS Session Timeout:

Security Groups (Select At Least One): NewRADIUSgroup RADIUS_Admins Radius_group

Cancel OK

f. Select **OK**.**Using the CLI:**

1. Define the RADIUS server:

```

config user radius
edit "FortiAuthenticator"
set secret ENC
6rF704/Zf3p2TutNyeSjPbQc73QrS21wNdmNXd/rg9k6nTR6yMhBRsJGpArhle6UOCb7b8In
M3nrCeuVETr/a02LpILmIltBq5sUMCNqbR6zp2fS3r35Eyd3IIrzmve4Vusi52c1MrCqVhzz
y2EfxkBrx5FhcRQWxStvnVt4+dzLYbHZ
set server "10.160.36.190"
next
end

```

2. Create a user group:

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

3. Configure the port security:

```
config switch interface
  edit "port1"
    set allowed-vlans 1
    config port-security
      set port-security-mode 802.1X
    end
    set security-groups "Radius_group"
  end
end
```

Example: dynamic VLAN

To assign VLAN dynamically for a port on which a user is authenticated, configure the RADIUS server attributes to return the VLAN ID when the user is authenticated. Assuming that the port security mode is set to 802.1X, the FortiSwitch unit will change the native VLAN of the port to the value returned by the server.

Ensure that the following attributes are configured on the RADIUS server:

- Tunnel-Private-Group-Id <integer or string> (the VLAN ID or VLAN name)
- Tunnel-Medium-Type IEEE-802 (6)
- Tunnel-Type VLAN (13)

NOTE: If the Tunnel-Private-Group-Id is set to the VLAN name, the same string must be specified in the `set description` command under the `config switch vlan` command.

Authenticating an admin user with RADIUS

If you want to use a RADIUS server to authenticate administrators, you must configure the authentication before you create the administrator accounts. Do the following:

1. Configure the FortiSwitch unit to access the RADIUS server.
2. Configure an administrator to authenticate with a RADIUS server and match the user secret to the RADIUS server entry.
3. Create the RADIUS user group.

Using the GUI:

1. Create a RADIUS system admin group:
 - a. Go to *System > Admin > Administrators*.
 - b. Select *Add Administrator*.
 - c. In the *Name* field, enter `RADIUS_Admins`.
 - d. Select *Remote*.
 - e. For the user group, select *Radius_group*.

- f. Select *Wildcard*.
- g. For the admin profile, select *super_admin*.

Add Administrator

Name	<input type="text" value="RADIUS_Admins"/>
Type	<input type="radio"/> Regular <input checked="" type="radio"/> Remote
User Group	<input type="text" value="Radius_group"/>
Wildcard	<input checked="" type="checkbox"/>
Override Profile	<input type="checkbox"/>
Backup Password	<input type="text"/>
Confirm Password	<input type="text"/>
Admin Profile	<input type="text" value="super_admin"/>
Scope	Global
	<input type="checkbox"/> Restrict this Admin Login from Trusted Hosts Only
	<input type="button" value="Cancel"/> <input type="button" value="Add"/>

- h. Select *Add*.
2. Create a user:
 - a. Go to *System > User > Definition*.
 - b. Select *Add User*.
 - c. In the *User Name* field, enter `RADIUS1`.
 - d. Select *Password* from the *Type* field.
 - e. In the *Password* field and *Confirm Password* field, enter
`6rF7O4/Zf3p2TutNyeSjPbQc73QrS21wNDmNXd/rg9k6nTR6yMhBRsJGpArhle6UOCb7b8InM3nr
 CeuVETr/a02LpILmIltBq5sUMCNqbR6zp2fS3r35Eyd3IIrzmve4Vusi52c1MrCqVhzy2EfxkBr
 x5FhcRQWxStvnVt4+dzLYbHZ.`

Add User

Username
 Enable
 Type v
 Password
 Confirm Password

- f. Select *Add*.
- 3. Create a user group:
 - a. Go to *System > User > Group*.
 - b. Select *Add Group*.
 - c. In the *Name* field, enter *RADIUS_Admins*.
 - d. Select *RADIUS1* in the Available Users box and select the right arrow to move it to the Members box.

Add Group

Name

Members

Available Users

Members

RADIUS1

Authentication Servers

Name	Group Name	Manage
No servers specified		

- e. Select *Add Group*.

Using the CLI:**1. Create 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
```

2. Create a user:

```
config user radius
  edit "RADIUS1"
    set secret ENC
      6rF704/Zf3p2TutNyeSjPbQc73QrS21wNDmNXd/rg9k6nTR6yMhBRsJGpArhle6UOCb7b8InM3n
      rCeuVETr/a02LpILmIltBq5sUMCNqbR6zp2fS3r35Eyd3IIrzmve4Vusi52c1MrCqVhzy2Efxk
      Brx5FhcRQWxStvnVt4+dzLYbHZ
  next
end
```

3. Create a user group:

```
config user group
  edit "RADIUS_Admins"
    set member "RADIUS1"
  next
end
```

RADIUS accounting and FortiGate RADIUS single sign-on

NOTE: To obtain a valid Framed-IP-Address attribute value, you need to manually configure DHCP snooping in the 802.1x-authenticated ports of your VLAN network for both port and MAC modes.

You can use your FortiSwitch unit for RADIUS single sign-on (RSSO) in two modes:

- Standalone mode
- FortiLink mode (FortiSwitch unit managed by FortiGate unit)

The FortiSwitch unit uses 802.1x-authenticated ports to send five types of RADIUS accounting messages to the RADIUS accounting server to support FortiGate RADIUS single sign-on:

- START—The FortiSwitch unit has been successfully authenticated, and the session has started.
- STOP—The FortiSwitch session has ended.
- INTERIM—Periodic messages sent based on the value set using the `set acct-interim-interval` command.
- ON—The FortiSwitch unit will send this message when the switch is turned on.
- OFF—The FortiSwitch unit will send this message when the switch is shut down.

NOTE: Starting in FortiSwitchOS 6.2.1, RADIUS accounting and CoA now support EAP and MAB 802.1x authentication.

Configuring the RADIUS accounting server and FortiGate RADIUS single sign-on

Use the following commands to set up RADIUS accounting and enable a FortiSwitch unit to receive CoA and disconnect messages from the RADIUS server:

```
config user radius
  edit <RADIUS_server_name>
    set acct-interim-interval <seconds>
    set secret <secret_key>
    set server <server_name_IPv4>
    config acct-server
      edit <entry_ID>
        set status {enable | disable}
        set server <server_IP_address>
        set secret <secret_key>
        set port <port_number>
      next
    end
  next
end
```

Variable	Description
<RADIUS_server_name>	Enter the name of the RADIUS server that will be sending CoA and disconnect messages to the FortiSwitch unit. By default, the messages use port 3799.
acct-interim-interval <seconds>	Enter the number of seconds between each interim accounting message sent to the RADIUS server. The value range is 60-86400. The default is 600.
secret <secret_key>	Enter the shared secret key for authentication with the RADIUS server.
server <server_name_IPv4>	Enter the domain name or IPv4 address for the RADIUS server. There is no default.
<entry_ID>	Enter the entry identifier. The value range is 0-20.
status {enable disable}	Enable or disable RADIUS accounting. The default is disable.
server <server_IP_address>	Enter the IPv4 address of the RADIUS server that will be receiving the accounting messages. There is no default value.
secret <secret_key>	Enter the shared secret key for the RADIUS accounting server.
port <port_number>	Enter the port number for the RADIUS accounting server to receive accounting messages from the FortiSwitch unit. The default is 1813.
source-ip <source_IP_address>	Enter the IPv4 address of the server that will be sending accounting messages. The default is 0.0.0.0.

Example: RADIUS accounting and single sign-on

Use the following commands to set up RADIUS accounting:

```

config user radius
  edit "local-RADIUS"
    set server 10.0.23.5
    set secret ENC
      LE8xetYYGiE0bkQpBDdH6acilwkYROCos7XK2q5cNPhu8sUDW9/fvkgE+fVURgZGEzTsndt4lgb+K+zV9m+nXCnoUXqivzQdt1UNlMxgKXADnCPxuiY966aJsYigmW/AZ1IM5kweUxvuHK8eqJkkT0nl64c8DID/LMAcCTx6JMapRCBS
    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 ENC
        LE8xetYYGiE0bkQpBDdH6acilwkYROCos7XK2q5cNPhu8sUDW9/fvkgE+fVURgZGEzTsndt4lgb+K+zV9m+nXCnoUXqivzQdt1UNlMxgKXADnCPxuiY966aJsYigmW/AZ1IM5kweUxvuHK8eqJkkT0nl64c8DID/LMAcCTx6JMapRCBS
      set port 1813
      set source-ip 10.105.142.19
    next
  end
next
end

```

RADIUS change of authorization (CoA)

NOTE: For increased security, each subnet interface that will be receiving CoA requests must be configured with the `set allowaccess radius-acct` command.

NOTE: Starting in FortiSwitchOS 6.2.1, RADIUS accounting and CoA support EAP and MAB 802.1x authentication.

The FortiSwitch unit supports two types of RADIUS messages:

- CoA messages to change session authorization attributes (such as data filters and the session-timeout setting) during an active session. To change the session timeout for an authenticated session, the CoA-Request message needs to use the IEEE session-timeout attribute.
- Disconnect messages (DMs) to flush an existing session. For MAC-based authentication, all other sessions are unchanged, and the port stays up. For port-based authentication, only one session is deleted.

RADIUS CoA messages use the following Fortinet proprietary attribute:

```
Fortinet-Host-Port-AVPair 42 string
```

The format of the value is as follows:

Attribute	Value	Description
Fortinet-Host-Port-AVPair	action=bounce-port	The FortiSwitch unit disconnects all sessions on a port. The port goes down for 10 seconds and then up again.
Fortinet-Host-Port-AVPair	action=disable-port	The FortiSwitch unit disconnects all session on a port. The port goes down until the user resets it.
Fortinet-Host-Port-AVPair	action=reauth-port	The FortiSwitch unit forces the reauthentication of the current session.

In addition, RADIUS CoA uses the session-timeout attribute:

Attribute	Value	Description
session-timeout	<session_timeout_value>	The FortiSwitch unit disconnects a session after the specified number of seconds of idleness. This value must be more than 60 seconds. NOTE: To use the session-timeout attribute, you must enable the <code>set radius-timeoutoverwrite</code> command first.

The FortiSwitch unit sends the following Error-Cause codes in RADIUS CoA-NAK and Disconnect-NAK messages:

Error Cause	Error Code	Description
Unsupported Attribute	401	This error is a fatal error, which is sent if a request contains an attribute that is not supported.
NAS Identification Mismatch	403	This error is a fatal error, which is sent if one or more NAS-Identifier Attributes do not match the identity of the NAS receiving the request.
Invalid Attribute Value	407	This error is a fatal error, which is sent if a CoA-Request or Disconnect-Request message contains an attribute with an unsupported value.
Session Context Not Found	503	This error is a fatal error if the session context identified in the CoA-Request or Disconnect-Request message does not exist on the NAS.

Configuring CoA and disconnect messages

Use the following commands to enable a FortiSwitch unit to receive CoA and disconnect messages from a RADIUS server:

```
config system interface
  edit "mgmt"
    set ip <address> <netmask>
```

```

    set allowaccess <access_types>
    set type physical
next
config user radius
  edit <RADIUS_server_name>
    set radius-coa {enable | disable}
    set radius-port <port_number>
    set secret <secret_key>
    set server <server_name_IPv4>
  end
end

```

Variable	Description
config system interface	
ip <address> <netmask>	Enter the interface IP address and netmask.
allowaccess <access_types>	Enter the types of management access permitted on this interface. Valid types are as follows: http https ping snmp ssh telnet radius-acct. Separate each type with a space. You must include radius-acct to receive CoA and disconnect messages.
<RADIUS_server_name>	Enter the name of the RADIUS server that will be sending CoA and disconnect messages to the FortiSwitch unit. By default, the messages use port 3799.
config user radius	
radius-coa {enable disable}	Enable or disable whether the FortiSwitch unit will accept CoA and disconnect messages. The default is disable.
radius-port <port_number>	Enter the RADIUS port number. By default, the value is 1812.
secret <secret_key>	Enter the shared secret key for authentication with the RADIUS server.
server <server_name_IPv4>	Enter the domain name or IPv4 address for the RADIUS server. There is no default.

Example: RADIUS CoA

The following example enables the FortiSwitch unit to receive CoA and disconnect messages from the specified RADIUS server:

```

config system interface
  edit "mgmt"
    set ip 10.105.4.14 255.255.255.0
    set allowaccess ping https http ssh snmp telnet radius-acct
    set type physical
  next
config user radius
  edit "Radius-188-200"
    set radius-coa enable

```

```

set secret ENC
+2NyBcp8JF3/OijWl/w5nOC++aDKQPWnlC8Ug2HKwn4RcmhqVYE+q07yI9eSDhtiIw63kR/oMBLGwF
QoeZf0QWengIlGTb+YQo/1YJn1V3Nwp9sdkcblfyayfc9gTeqe+mFltKl5IWNI7WRYiJC8sxaF9Iyr
2/14hpCiVUMiPOU6fSrj
set server "10.105.188.200"
next
end

```

Viewing the CoA configuration

Use the following command to check the CoA settings:

```

S524DF4K15000024 # diagnose user radius coa

90075.874 DAS: :radius_das_diag_handler:
RADIUS DAS Server List:
radius2:
Type: RADIUS_8021X, IP: 10.105.252.79,
Last CoA/DM Client IP Addr      : 10.105.252.79
Disc Reqs      : 2
Disc ACKs      : 1
Disc NAKs      : 1
CoA Reqs       : 0
CoA ACKs       : 0
CoA NAKs       : 0
radius3:
Type: RADIUS_8021X, IP: 10.105.252.76,
Last CoA/DM Client IP Addr      :
Disc Reqs      : 0
Disc ACKs      : 0
Disc NAKs      : 0
CoA Reqs       : 0
CoA ACKs       : 0
CoA NAKs       : 0

```

Use cases

Here are three use cases for 802.1x authentication.

Use case 1

In this use case, a Cisco phone uses MAB and uses LLDP-MED to assign the voice VLAN. A PC behind the Cisco phone uses 802.1x authentication with or without dynamic VLAN assignment.

The following is an example configuration:

```

config switch lldp profile
edit "lldp-cisco-104"
set 802.1-tlvs port-vlan-id
set 802.3-tlvs power-negotiation
config med-network-policy
edit "voice"
set assign-vlan enable

```

```

        set status enable
        set vlan 104
    next
    set med-tlvs inventory-management network-policy
next
end

config switch physical-port
edit "port1"
    set lldp-profile "lldp-cisco-104"
next
end

config switch interface
edit "port1"
    set native-vlan 20
    set security-groups "CISEGRP"
    set snmp-index 1
    config port-security
        set mac-auth-bypass enable // Required. You need to enable MAB.
        set port-security-mode 802.1X-mac-based // Required
    end
next
end

```

Use case 2

In this use case, the Cisco phone uses 802.1x authentication and uses LLDP-MED to assign the voice VLAN. A PC behind the Cisco phone uses 802.1x authentication without dynamic VLAN assignment.

RADIUS dynamic VLAN assignment for the voice VLAN must match the voice VLAN configured in the LLDP-MED profile for Cisco phone 802.1x authentication.

The following is an example configuration:

```

config switch lldp profile
edit "lldp-cisco-104"
    set 802.1-tlvs port-vlan-id
    set 802.3-tlvs power-negotiation
    config med-network-policy
        edit "voice"
            set assign-vlan enable
            set status enable
            set vlan 104
        next
    set med-tlvs inventory-management network-policy
next
end

config switch physical-port
edit "port1"
    set lldp-profile "lldp-cisco-104"
next
end

config switch interface
edit "port1"

```

```

set native-vlan 20
set security-groups "CISEGRP"
set snmp-index 1
  config port-security
    set mac-auth-bypass disable // Optional
    set eap-auto-untagged-vlans disable // Required. Needed to allow voice
      traffic with voice VLAN tag at egress
    set port-security-mode 802.1X-mac-based // Required
  end
next
end

```

Use case 3

In this use case, the Cisco phone uses 802.1x authentication and uses LLDP-MED to assign the voice VLAN. The PC behind the Cisco phone uses 802.1x authentication with dynamic VLAN assignment.

RADIUS dynamic VLAN assignment for the voice VLAN has to match the voice VLAN configured in the LLDP-MED profile for Cisco phone 802.1x authentication.

The VLAN ID from the RADIUS dynamic VLAN assignment for the PC has to be added in the untagged VLAN list on the port.

The following is an example configuration:

```

config switch lldp profile
  edit "lldp-cisco-104"
    set 802.1-tlvs port-vlan-id
    set 802.3-tlvs power-negotiation
    config med-network-policy
      edit "voice"
        set assign-vlan enable
        set status enable
        set vlan 104
      next
    set med-tlvs inventory-management network-policy
  next
end

config switch physical-port
  edit "port1"
    set lldp-profile "lldp-cisco-104"
  next
end

config switch interface
  edit "port1"
    set native-vlan 20
    set allowed-vlans 50 60 70 // Assume that VLANs 50, 60, and 70 are a part of the
      dynamic VLANs configured on RADIUS for PCs in different groups.
    set untagged-vlans 50 60 70
    set security-groups "CISEGRP"
    set snmp-index 1
    config port-security
      set mac-auth-bypass disable // Optional
      set eap-auto-untagged-vlans disable // Required. Needed to allow voice
        traffic with voice VLAN tag at egress
      set port-security-mode 802.1X-mac-based // Required
    end
  end
end

```

```
    end
  next
end
```

Detailed deployment notes

- Using more than one security group (with the `set security-groups` command) per security profile is not supported.
- CoA and single sign-on are supported only by the CLI in this release.
- RADIUS CoA is supported in standalone mode and in non-NAT FortiLink mode.
- The FortiSwitch unit supports using FortiAuthenticator, FortiConnect, Microsoft Network Policy Server (NPS), Aruba ClearPass, and Cisco Identity Services Engine (ISE) as the RADIUS server for CoA and RSSO.
- Each RADIUS CoA server can support only one accounting manager in this release.
- RADIUS accounting/CoA/VLAN-by-name features are supported only with `eap-passthru enable`.
- Fortinet recommends a unique secret key for each accounting server.
- For CoA to correctly function with FortiAuthenticator or FortiConnect, you must include the User-Name attribute (you can optionally include the Framed-IP-Address attribute) *or* the User-Name and Calling-Station-ID attributes in the CoA request.
- To obtain a valid Framed-IP-Address attribute value, you need to manually configure DHCP snooping in the 802.1x-authenticated ports of your VLAN network for both port and MAC modes.
- Port-based basic statistics for RADIUS accounting messages are supported in the Accounting Stop request.
- By default, the accounting server is disabled. You must enable the accounting server with the `set status enable` command.
- The default port for FortiAuthenticator single sign-on is 1813 for the FortiSwitch unit.
- In MAC-based authentication, the maximum number of client MAC addresses is 20. Each model has its own maximum limit.
- Static MAC addresses and sticky MAC addresses are mechanisms for manual/local authorization; 802.1x is a mechanism for protocol-based authorization. Do not mix them.
- Fortinet recommends an 802.1x setup rate of 5 to 10 sessions per second.
- Starting in FortiSwitch 6.2.0, when 802.1x authentication is configured, the EAP pass-through mode (`set eap-passthru`) is enabled by default.
- For information about RADIUS attributes supported by FortiSwitchOS, refer to the “Supported attributes for RADIUS CoA and RSSO” appendix.
- In general for 802.1x deployment, Fortinet suggests disabling STP in the 802.1x security ports. If STP is enabled on the ports, the ports must be assigned to STP instances that belong to a dynamic VLAN, guest VLAN, or auth-fail VLAN; otherwise, the network connectivity fails after the ports are authorized and assigned to a dynamic VLAN, guest VLAN, or auth-fail VLAN.

TACACS

This chapter contains information on using Terminal Access Controller Access-Control System (TACACS+) authentication with your FortiSwitch unit.

This chapter covers the following topics:

- [Administrative accounts on page 270](#)
- [User accounts on page 271](#)
- [Example configuration on page 271](#)

Administrative accounts

Administrative, or admin, accounts allow access to various aspects of the FortiSwitch configuration. The level of access is determined by the admin profile that is assigned to the admin account.

See [Configuring administrator tasks on page 32](#) for the steps to create an admin profile.

Configuring a TACACS admin account

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices using one or more centralized servers. If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiSwitch unit contacts the TACACS+ server for authentication.

Using the GUI:

1. Go to *System > Admin > Administrators* and select *Add Administrator*.
2. Give the administrator account an appropriate name.
3. Select *Remote* for the administrator type.
4. Select a user group for remote users.
5. Enable *Wildcard*.
6. Select an administrator profile.
7. Select *Add*.

Using the CLI:

```
config system admin
  edit tacuser
    set remote-auth enable
    set wildcard enable
    set remote-group <group>
    set accprofile <profile>
  end
end
```

User accounts

User accounts identify a network user and determine what parts of the network the user is allowed to access.

Configuring a user account

```
config user tacacs+
  edit <tacserver>
    set authen-type {ascii | auto | chap | ms_chap | pap}
    set authorization enable
    set key <authorization_key>
    set server <server>
  end
end
```

Configuring a user group

```
config user group
  edit <tacgroup>
    set member <tacserver>
    config match
      edit 1
        set server-name <server>
        set group-name <group>
      end
    end
  end
end
```

Example configuration

The following is an example configuration of a TACACS+ user account, with the CLI syntax shown to create it:

1. Configuring 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
```

2. Configuring a TACACS+user group:

```
config user group
  edit tacgroup
    set member tacserver
    config match
      edit 1
        set server-name tacserver
        set group-name tacgroup
      end
    end
```

```
    end
  end
end
```

3. Configuring a TACACS+ system admin user account:

```
config system admin
  edit tacuser
    set remote-auth enable
    set wildcard enable
    set remote-group tacgroup
    set accprofile noaccess
  end
end
```

Troubleshooting and support

The FortiSwitch unit provides various features for troubleshooting and support.

This chapter covers the following topics:

- [Dashboard on page 273](#)
- [Virtual wire on page 276](#)
- [TFTP network port on page 277](#)
- [Cable diagnostics on page 277](#)
- [Selective packet sampling on page 278](#)
- [Packet capture on page 279](#)
- [Network monitoring on page 281](#)
- [Flow tracking and export on page 284](#)
- [Identifying a specific FortiSwitch unit on page 287](#)

Dashboard

The dashboard displays your FortiSwitch management mode and shows the current values for the following:

- CPU
- RAM
- Temperature for FortiSwitch models that have temperature sensors
- PoE (on FortiSwitch PoE models)
- Bandwidth
- Losses

Operation mode


The Operation Mode field shows whether the FortiSwitch unit is managed by a FortiGate unit.

When the FortiSwitch unit is in FortiLink mode, a message is displayed above the dashboard, and the Operation Mode is “Remote Management.”

The screenshot shows a warning banner at the top: "This FortiSwitch is managed by FortiLink. Local changes are not recommended." Below this is the "Dashboard" header and a "System Information" section. The "System Information" section contains the following details:

Serial Number	S524DF4K15000024	System Configuration	Last Backup: Never [Backup] [Restore] [Revisions]
BIOS Version	04000018	System Time	Fri Jun 14th 2019 02:35:32 PM [Change]
Firmware Version	v6.2.0,build0175,190610 (Interim) [Upgrade]	Uptime	4 Days, 1 Hour, 6 Minutes [Reboot] [Shut Down]
Current Administrator	admin [Change Password]/1 in Total [Details]	Current License	enhanced-debugging, FS-SW-LIC-500 [Change]
Operation Mode	Remote Management	FortiSwitchCloud	Disconnected


When the FortiSwitch unit is in standalone mode, the Operation Mode is “Local Management.”

System Information			
Serial Number	S548DF5018000776	System Configuration	Last Backup: Never [Backup] [Restore] [Revisions]
BIOS Version	04000018	System Time	Fri Jun 14th 2019 02:45:25 PM [Change]
Firmware Version	v6.2.0,build0175,=190613= (Interim) [Upgrade]	Uptime	0 Days, 3 Hours, 53 Minutes [Reboot] [Shut Down]
Current Administrator	admin [Change Password] /1 in Total [Details]	Current License	enhanced-debugging, FS-SW-LIC-500 [Change]
Operation Mode	Local Management	FortiSwitchCloud	 Connected

Select *Remote Management* or *Local Management* to go to the Management Mode page, where you can switch between FortiLink mode and standalone mode.

FortiSwitch Cloud

The FortiSwitchCloud field shows whether the FortiSwitch unit is managed by FortiSwitch Cloud. A FortiSwitch unit must be in standalone mode to be managed by FortiSwitch Cloud. For more details about using FortiSwitch Cloud, refer to the *FortiSwitch Cloud Administration Guide*.

System Information			
Serial Number	S548DF5018000776	System Configuration	Last Backup: Never [Backup] [Restore] [Revisions]
BIOS Version	04000018	System Time	Fri Jun 14th 2019 02:51:35 PM [Change]
Firmware Version	v6.2.0,build0175,=190613= (Interim) [Upgrade]	Uptime	0 Days, 3 Hours, 59 Minutes [Reboot] [Shut Down]
Current Administrator	admin [Change Password] /1 in Total [Details]	Current License	enhanced-debugging, FS-SW-LIC-500 [Change]
Operation Mode	Local Management	FortiSwitchCloud	 Connected

Select *Connected* or *Disconnected* to go to the *System > FortiSwitchCloud* page.

FortiSwitchCloud

Status	Disconnected: Unable to Connect to Service. Please wait...
<input type="checkbox"/> Enable	
	Update

Select *Enable* and then select *Advanced Settings* to configure your FortiSwitch unit to be managed by FortiSwitch Cloud.

FortiSwitchCloud

Status Disconnected: Unable to Connect to Service.
Please wait...

Enable

▼ **Advanced Settings**

Name	fortiswitch-dispatch.forticloud.com	
Port	443	(1-65535)
Interval (Seconds)	3	(3-300)

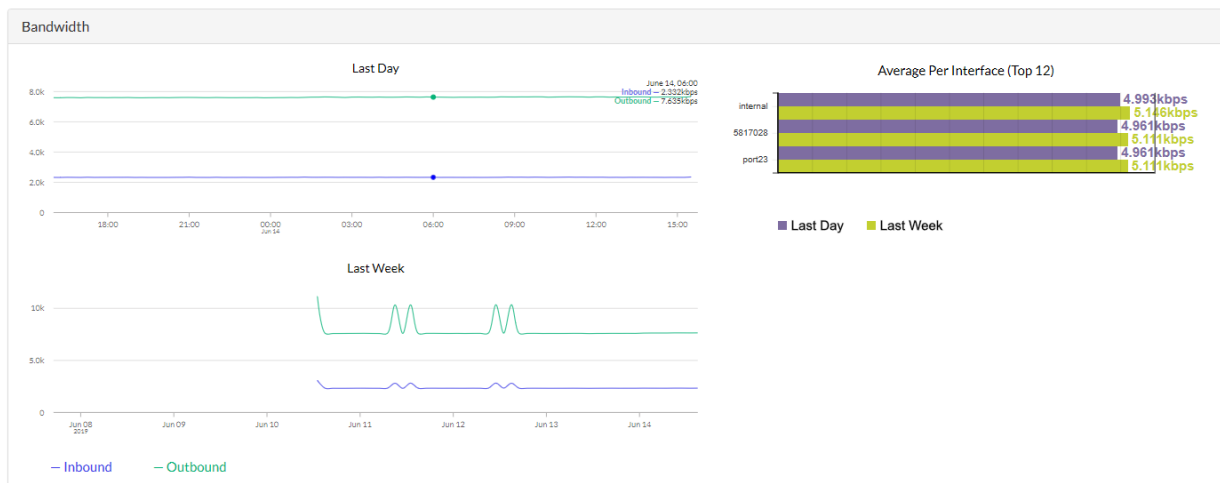
Update

To switch to FortiSwitch Cloud management:

1. On the FortiSwitchCloud page, select *Enable* and then select *Advanced Settings*.
2. By default, the Name field is set to `fortiswitch-dispatch.forticloud.com`, the domain name for FortiSwitch Cloud. No change is needed.
3. By default, the Port field is set to 443, the port number used to connect to FortiSwitch Cloud. No change is needed.
4. In the Interval (Seconds) field, enter the time in seconds allowed for domain name system (DNS) resolution. The default is 15 seconds. The range of values is 3-300 seconds.
5. Select *Update* to save your changes.

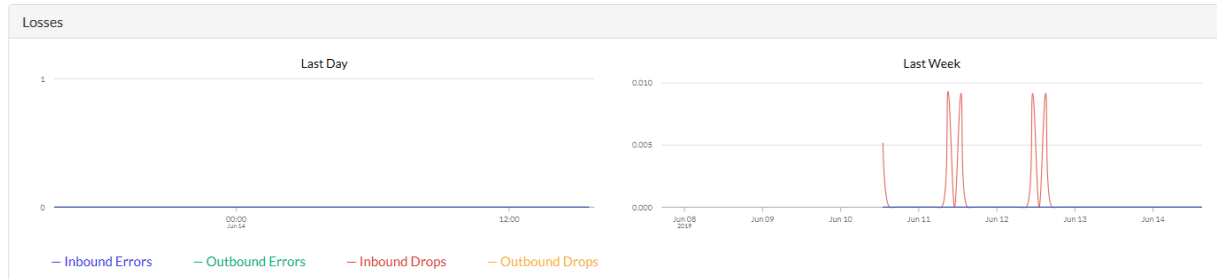
Bandwidth

The Bandwidth graphs show the inbound and outbound bandwidth for the entire FortiSwitch unit over a day and over a week. The Average Per Interface bar chart shows the average bandwidth (inbound bandwidth plus outbound bandwidth) for each interface over a day and over a week; only the interfaces with the highest bandwidth are displayed.



Losses

The Losses graphs show the inbound errors, outbound errors, inbound drops, and outbound drops for the entire FortiSwitch unit over a day and over a week.



Virtual wire

Some testing scenarios might require two ports to be wired 'back-to-back'. Instead of using a physical cable, you can configure a virtual wire between two ports. The virtual wire forwards traffic from one port to the other port with minimal filtering or modification of the packets.

Notes:

- ACL mirroring is not supported.
- You can select ports that are already ingress and egress mirror sources.

Using the GUI:

1. Go to *Switch > Virtual Wires*.
2. Select *Add Virtual Wire* to create a new virtual wire.
3. Enter a name and select the ports for first member and second member.
4. Select *Add* to save the changes.

Using the CLI:

Use the following commands to configure a virtual wire:

```
config switch virtual-wire
  edit <virtual-wire-name>
    set first-member <port-name>
    set second-member <port-name>
    set vlan <vlan-id>
  next
end
```

Virtual wire ports set a special Tag Protocol Identifier (TPID) in the VLAN header. The default value is 0xdee5, a value that real network traffic never uses.

Use the following commands to configure a value for the TPID:

```
config switch global
  set virtual-wire-tpid <hex value from 0x0001 to 0xFFFFE>
```

```
end
```

Use the following command to display the virtual wire configuration:

```
diagnose switch physical-ports virtual-wire list
```

```
port1(1) to port2(2) TPID: 0xdee5 VLAN: 4011
port3(3) to port4(4) TPID: 0xdee5 VLAN: 4011
port5(5) to port25(25) TPID: 0xdee5 VLAN: 4011
port7(7) to port8(8) TPID: 0xdee5 VLAN: 4011
```

Note the following information about virtual wire:

- Ports have ingress and egress VLAN filtering disabled. All traffic (including VLAN headers) is passed unchanged to the peer. All egress traffic is untagged.
- Ports have L2 learning disabled.
- Ports have their egress limited to their peer and do not allow egress from any other ports.
- The system uses TCAM to force forwarding from a port to its peer.
- The TCAM prevents any copy-to-cpu or packet drops.

TFTP network port

When you power on the FortiSwitch unit, the BIOS performs basic device initialization. When this activity is complete, and before the OS starts to boot, you can click any key to bring up the boot menu.

From the menu, click the "I" key to configure TFTP settings. With newer versions of the BIOS, you can specify the network port (where you have connected your network cable). If you are not prompted to specify the network port, you must connect your network cable to the default network port:

- If the switch model has a WAN port, the WAN port is the network port.
- If the switch has no WAN port, the highest port number is the network port.

Cable diagnostics

You can check the state of cables connected to a specific port. The following pair states are supported:

- Open
- Short
- Ok
- Open_Short
- Unknown
- Crosstalk

If no cable is connected to the specific port, the state is Open, and the cable length is 0 meters.

For supported models, see [Supported models on page 13](#).

Using the GUI:

1. Go to *Switch > Port > Physical*.
2. Select *Cable Diagnostic* for the appropriate port.
3. Select *Continue* to start the cable diagnostics.
NOTE: Running cable diagnostics on a port that has the link up will interrupt the traffic for several seconds.
4. Select *Back to Physical Ports* to close the Cable Diagnostics window.

Using the CLI:

Use the following command to run a time domain reflectometry (TDR) diagnostic test on cables connected to a specific port:

```
diagnose switch physical-ports cable-diag <physical port name>
```

NOTE: Running cable diagnostics on a port that has the link up will interrupt the traffic for several seconds.

For example:

```
# 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
```

Use the following command to check the medium dependent interface crossover (MDI-X) interface status for a specific port:

```
diagnose switch physical-ports mdix-status <physical port name>
```

For example:

```
# diagnose switch physical-ports mdix-status port1

port1: MDIX(Crossover)
```

Selective packet sampling

NOTE: This feature is not supported on 3032.

During debugging, you might want to see whether a particular type of packet was received on an interface on the switch.

1. Set up an access control list (ACL) on the switch with the interface that you want to monitor. See [Access control lists on page 139](#). This ACL is the ingress interface.
2. Set up a mirror for the “internal” interface.

For example, if you want to monitor interface port17 for any IP packet (ether-type 0x800) with a destination subnet of 10.10.10/24 and a source subnet of 20.20.20/24, use the following commands.

```
# show switch acl ingress
config switch acl ingress
edit 1
```

```

config action
  set mirror "internal"
end
config classifier
  set dst-ip-prefix 10.10.10.0 255.255.255.0
  set ether-type 0x0800
  set src-ip-prefix 20.20.20.0 255.255.255.0
end
set ingress-interface "port17"
set status active
next
end
    
```

To examine the packets that have been sampled in the example, use the following command:

```
# diagnose sniffer packet sp17 none 6
```

Packet capture

When troubleshooting networks, it helps to look inside the header of the packets. This helps to determine if the packets, route, and destination are all what you expect. Packet capture is also called a network tap, packet sniffing, or logic analyzing.

To capture packets:

1. Create a packet-capture profile.
2. Start the packet capture.
3. Pause or stop the packet capture.
4. Display or upload the packet capture.
5. Delete the packet-capture file.

The maximum number of packet-capture profiles and the RAM disk size allotted for packet capture are different for the various platforms:

Platform	Maximum number of profiles	RAM disk size in MB
1xx	8	20
2xx	8	50
4xx	16	75
5xx	16	100
1xxx	16	100
3xxx	16	100

Create a packet-capture profile

To specify which packets to capture, define a filter and select a switch or system interface on which to capture the packets. You cannot select both a switch interface and a system interface.

The filter uses flexible logic. For example, if you want packets using UDP port 1812 between hosts named `forti1` and either `forti2` or `forti3`:

```
'udp and port 1812 and host forti1 and \( forti2 or forti3 \)'
```

You can specify the number of packets to capture and the maximum packet length to be captured. The maximum number of packets that can be captured depends on the RAM disk size.

To create a packet-capture profile:

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

For example:

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

Start the packet capture

Use the following command to start running a packet capture with an already configured packet-capture profile:

```
execute system sniffer-profile start <profile-name>
```

For example:

```
execute system sniffer-profile start profile1
```

Pause or stop the packet capture

A packet capture continues to run until the `max-pkt-cnt` value is reached or a command is entered to pause or stop the packet capture. To restart a paused packet capture, use the `execute system sniffer-profile start <profile-name>` command.

To pause the packet capture:

```
execute system sniffer-profile pause <profile_name>
```

To stop the packet capture:

```
execute system sniffer-profile stop <profile-name>
```

Display or upload the packet capture

You can display parsed information from the packet capture or upload the .pcap file to a TFTP or FTP server for further analysis.

To display the packet capture from a specific packet-capture profile:

```
get system sniffer-profile capture <profile_name>
```

To upload the .pcap file for a specific packet-capture profile to an FTP server:

```
execute system sniffer-profile upload ftp <profile_name> <packet_capture_file_
name.pcap> <FTP_server_IP_address:<optional_port>>
```

To upload the .pcap file for a specific packet-capture profile to a TFTP server:

```
execute system sniffer-profile upload tftp <profile_name> <packet_capture_file_
name.pcap> <TFTP_server_IP_address:<optional_port>>
```

Delete the packet-capture file

After you have examined the packet capture, you can manually delete the .pcap file. You can only delete the .pcap after the packet capture is stopped. You cannot delete the .pcap file if the packet capture is paused or running. All .pcap files are deleted when you power cycle the switch.

To delete the .pcap file for a specific packet-capture profile:

```
execute system sniffer-profile delete-capture <profile_name>
```

For example:

```
execute system sniffer-profile delete-capture profile1
```

Network monitoring

You can monitor specific unicast MAC addresses in directed mode, monitor all detected MAC addresses on a FortiSwitch unit in survey mode, or do both. The FortiSwitch unit gives the directed mode a higher priority than survey mode. The directed mode and survey mode are disabled by default.

NOTE: Network monitoring is not available on FSR-112D-POE.

Directed mode

In directed mode, you select which unicast MAC addresses that you want examined. The FortiSwitch unit detects various fields of the packet—such as MAC address, IP address, VLAN, and user name—and stores the data in either of two databases.

NOTE: You cannot specify broadcast or multicast MAC addresses.

The maximum number of MAC addresses that can be monitored depends on the FortiSwitch model.

Platform Series	Maximum Number of MAC Addresses Monitored	Maximum Number of Hosts
1xx, 2xx	10	250
4xx, 5xx	20	1,024
10xx, 30xx	30	4,096

To find out how many network monitors are available, use the following command:

```
diagnose switch network-monitor cfg-stats
```

```
Network Monitor Configuration Statistics:
```

```
-----
```

```
Adds          : 0
Deletes        : 0
Free Entries   : 20
```

To find out which network monitors are being used currently, use the following command:

```
diagnose switch network-monitor dump-monitors
```

Entry ID	Monitor Type	Monitor MAC	Packet-count
1	directed-mode	00:01:02:03:04:05	10
2	directed-mode	10:01:02:03:04:05	0
3	survey-mode	08:5b:0e:c1:07:65	419
4	survey-mode	08:5b:0e:4f:af:38	101
5	survey-mode	08:5b:0e:ce:59:40	2347
6	survey-mode	08:5b:0e:4f:af:44	0
7	survey-mode	08:5b:0e:c1:07:65	0
8	survey-mode	08:5b:0e:4f:af:38	80
9	survey-mode	08:5b:0e:ce:59:40	117
10	survey-mode	08:5b:0e:4f:af:44	0

To start network monitoring, use the following commands:

```
config switch network-monitor settings
  set status enable
end
```

To specify a single unicast MAC address (formatted like this: xx:xx:xx:xx:xx:xx) to be monitored, use the following commands:

```
config switch network-monitor directed
  edit <unused network monitor>
    set monitor-mac <MAC address>
  next
end
```

For example:

```
config switch network-monitor directed
```

```

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

Survey mode

In survey mode, the FortiSwitch unit detects MAC addresses to monitor for a specified number of seconds. You can specify network monitoring for 120 to 3,600 seconds. The default time is 120 seconds. The FortiSwitch unit detects various fields of the packet—such as MAC address, IP address, VLAN, and user name—and stores the data in either of two databases.

To start network monitoring in survey mode, use the following commands:

```

config switch network-monitor settings
    set status enable
    set survey-mode enable
    set survey-mode-interval <120-3600 seconds>
end
    
```

For example:

```

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

Network monitoring statistics

After you have enabled network monitoring, you can view the statistics for the number and types of packets.

To see the type of packets going to and from monitored MAC addresses, use the following command:

```
diagnose switch network-monitor parser-stats
```

```
Network Monitor Parser Statistics:
```

```

-----
Arp           : 0
Ip            : 1
Udp           : 46
Tcp           : 353
Dhcp          : 0
Eapol        : 0
Unsupported  : 352
    
```

To see the number of packets going to and from monitored MAC addresses, use the following command:

```
diagnose switch network-monitor dump-monitors
```

Entry ID	Monitor Type	Monitor MAC	Packet-count
1	directed-mode	00:01:02:03:04:05	10
2	directed-mode	10:01:02:03:04:05	0
3	survey-mode	08:5b:0e:c1:07:65	419
4	survey-mode	08:5b:0e:4f:af:38	101

5	survey-mode	08:5b:0e:ce:59:40	2347
6	survey-mode	08:5b:0e:4f:af:44	0
7	survey-mode	08:5b:0e:c1:07:65	0
8	survey-mode	08:5b:0e:4f:af:38	80
9	survey-mode	08:5b:0e:ce:59:40	117
10	survey-mode	08:5b:0e:4f:af:44	0

NOTE: The FortiSwitch unit creates an entry in the layer-3 database using the exact packet contents when they were parsed. If the MAC address is then assigned to a different VLAN, this change might not be detected immediately. If there is a discrepancy in the output for the `diagnose switch network-monitor dump-l2-db` and `diagnose switch network-monitor dump-l3-db` commands, use the output with the more recent time stamp.

To see all detected devices from the layer-2 database, use the following command:

```
diagnose switch network-monitor dump-l2-db

mac 00:01:02:03:04:05 vlan 1
created 19 secs ago, last seen 16 secs ago
user JoE sources: eapol
```

To see all detected devices from the IP address database, use the following command:

```
diagnose switch network-monitor dump-l3-db

mac 08:5b:0e:c1:07:65 ip 169.254.2.2 vlan 4094
created 63614 secs ago, last seen 2 secs ago
sources: arp ip
mac 00:10:20:30:40:50 ip 10.10.10.111 vlan 123
created 75 secs ago, last seen 45 secs ago
sources: arp ip
mac 00:11:22:33:44:55 ip 30.30.30.115 vlan 1
created 53 secs ago, last seen 53 secs ago
sources: dhcp arp ip
```

Flow tracking and export

NOTE:

- Flow export is supported on FortiSwitch models 2xx and higher.
- Layer-2 flows for netflow 1 and netflow 5 are not supported.

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.

To use flow export, you need to enable packet sampling and then configure the flow export.

Enabling packet sampling

To use flow export, you must first enable packet sampling for each switch port and trunk:

```

config switch interface
  edit <interface>
    set packet-sampler enabled
    set packet-sample-rate <0-99999>
  end

```

Configuring flow export

```

config system flow-export
  set collector-ip <IPv4_address>
  set collector-port <port_number>
  set format {netflow1 | netflow5 | netflow9 | ipfix}
  set identity <hexadecimal>
  set level {ip | mac | port | proto | vlan}
  set max-export-pkt-size <integer>
  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>
  set transport {sctp | tcp | udp}
config aggregates
  edit <id>
    set ip <IPv4_address_mask>
  end
end

```

Variable	Description	Default
collector-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
collector-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
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. NOTE: 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 v5 set the sample rate consistently across all ports.	netflow9

Variable	Description	Default
identity <hexadecimal>	Required. Enter a unique number to identify which FortiSwitch unit the data originates from. The range of values is 0x00000000-0xFFFFFFFF. If <code>identity</code> is not specified, the “Burn in MAC” value is used instead (see <code>get system status</code>).	0x00000000
level {ip mac port proto vlan}	You can set the flow-tracking level to one of the following: <ul style="list-style-type: none"> - <code>ip</code>—The FortiSwitch unit collects the source IP address and destination IP address from the sample packet. - <code>mac</code>—The FortiSwitch unit collects the source MAC address and destination MAC address from the sample packet. - <code>port</code>—The FortiSwitch unit collects the source IP address, destination IP address, source port, destination port, and protocol from the sample packet. - <code>proto</code>—The FortiSwitch unit collects the source IP address, destination IP address, and protocol from the sample packet. - <code>vlan</code>—The FortiSwitch unit collects the source IP address, destination IP address, source port, destination port, protocol, and VLAN from the sample packet. 	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
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
transport {sctp tcp udp}	You can set exported packets to use UDP, TCP, or SCTP for transport.	udp

Variable	Description	Default
<id>	Enter the identifier.	No default
<IPv4_address_mask>	Enter the IPv4 address and mask to match. All matching sessions will be aggregated into the same flow.	No default

Viewing the flow-export data

You can display the flow-export data or raw data for a specified number of records or for all records. You can also display statistics for flow-export data.

```
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.

Deleting the flow-export data

Use the following commands to delete or expire all flow-export data:

```
diagnose sys flow-export delete-flows-all
diagnose sys flow-export expire-flows-all
```

Identifying a specific FortiSwitch unit

When you have multiple FortiSwitch units and need to locate a specific switch, use the following command to flash all port LEDs on and off for a specified number of minutes:

```
diagnose switch physical-ports led-flash <disable | time>
```

You can flash the port LEDs for 5, 15, 30, or 60 minutes. After you locate the FortiSwitch unit, you can use `disable` to stop the LEDs from flashing.

NOTE: For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.


```
    next
end
```

5. Configure port security on the dot1x port.

- a. Configure mac-mode port-security.
- b. Add voice VLAN on allowed list (for example, 21).
- c. Apply the security group.

Interface port4 configuration:

```
# show switch interface port4
config switch interface

    edit "port4"
    set allowed-vlans 20-21,31,41
    set security-groups "Corp_Grp_10"
    set snmp-index 4
configure port-security
    set auth-fail-vlan disable
    set guest-auth-delay 120
    set guest-vlan disable
    set mac-auth-bypass enable
    set port-security-mode 802.1X-mac-based
    set radius-timeout-overwrite disable
    set auth-fail-vlanid 40
    set guest-vlanid 30
end
```

RADIUS configuration

MAB Authentication:

- Add phone MAC address to MAB list.

802.1X Authentication

1. Create a local user.
2. Create a user group with "Attributes" and enable PEAP and MSChapv2.

DHCP configuration

1. On the DHCP server, configure a pool for phone and a pool for the PC.

```
!
ip dhcp pool PC
network 10.1.1.0 255.255.255.0
default-router 10.1.1.1
dns-server 10.1.1.1
!
ip dhcp pool PC
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
dns-server 20.1.1.5
```

2. Configure exclude lists for pools for both gateway and DNS.

```
ip dhcp excluded-address 20.1.1.1 20.1.1.1.5
<<<<gateway and dns server
ip dhcp excluded-address 10.1.1.1 10.1.1.1.5
<<<<gateway and dns server
!
ip dhcp pool PC
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
dns-server 20.1.1.5
```

3. Configure the switch port VLAN interface as a gateway for the phone.

```
# show run
Building configuration

Current configuration
!
interface vlan21 <<<<<<
ip address 20.1.1.1
end
```

4. Configure the switch port VLAN interface as a gateway for the PC.

```
# show run
Building configuration

Current configuration
!
interface vlan10 <<<<<<
ip address 10.1.1.1
end

#
```

5. Configure the I2 port and associate the voice VLAN.

```
# show run
Building configuration

Current configuration
!
interface GigabitEthernet g1/0/1 <<<<<<
switchport access vlan 21
switchport trunk encapsulation dot1q
switchport trunk all
switchport mode trunk
end
```

6. Configure the I2 port and associate the data VLAN.

```
# show run
Building configuration

Current configuration
!
```


edited on: 2016-11-29 17:25

edited on: 2016-11-29 17:59

- b. On the PC, verify that the DHCP address is assigned.
- c. From the DHCP server, check the binding and a ping from gateway to verify that the PC is reachable.

Appendix: FortiSwitch-supported RFCs

RFC 3289

Description:

DIFFSERV-DSCP-TC.
DIFFSERV-MIB.
QOS-DIFFSERV-EXTENSIONS-MIB.
QOS-DIFFSERV-PRIVATE-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc3289>

RFC 2934

Description:

PIM-MIB.
DVMRP-STD-MIB.
IANA-RTPROTO-MIB.
MULTICAST-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc2934>

RFC 2932

Description:

IPMROUTE-MIB.
Fortinet Enterprise MIB.
ROUTING-MIB.
MGMD-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc2932>

RFC 2819

Description:

Remote Network Monitoring Management Information Base.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc2819>

RFC 2787

Description:

Definitions of Managed Objects for the Virtual Router Redundancy Protocol.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc2787>

RFC 2674

Description:

Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc2674>

RFC 2620

Description:

Radius-Acc-Client-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc2620>

RFC 2618

Description:

Radius-Auth-Client-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc2618>

RFC 2576

Description:

Coexistence between SNMPs.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc2576>

RFC 2573

Description:

SNMP Applications.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc2573>

RFC 2572

Description:

Message Processing for SNMP.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc2572>

RFC 2571

Description:

SNMP Frameworks.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc2571>

RFC 2362

Description:

Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification.

Category:

Router (PIM SM)

Web page

<http://tools.ietf.org/html/rfc2362>

RFC 2328

Description:

OSPF version 2.

Category:

OSPF

Web page

<http://tools.ietf.org/html/rfc2328>

RFC 2233

Description:

Interface MIB.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc2233>

RFC 1850

Description:

OSPF-TRAP-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc1850>

RFC 1724

Description:

RIPv2-MIB.

Category:

MIB

Web page

<http://tools.ietf.org/html/rfc1724>

RFC 1643

Description:

Ether-like MIB.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc1643>

RFC 1583

Description:

OSPF version 2.

Category:

OSPF

Web page

<http://tools.ietf.org/html/rfc1583>

RFC 1493

Description:

Bridge.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc1493>

RFC 1213

Description:

MIB II parts that apply to FortiSwitch 100 units.

Category:

SNMP

Web page

<http://tools.ietf.org/html/rfc1213>

Appendix: Supported attributes for RADIUS CoA and RSSO

Attributes sent from the FortiSwitch unit to the RADIUS server during 802.1x authentication (Access-Request)

Attribute	AVP Type	Type	Description
NAS-Identifier	32	text	Host name of switch
User-Name	1	alphanumeric	User name of supplicant or MAC address
EAP-Message	79	concat	Include EAP content
Framed-MTU	12	integer	Configurable (size of bytes). The range of values is 600-1500. The default value is 1500.
NAS-Port-Id	87	text	Port connected to supplicant
NAS-Port	5	integer	Value of port ID; for example, 12 means port12
NAS-Port-Type	61	enum	Ethernet (15)
Calling-Station-ID	31	text	MAC address of supplicant
Message-Authenticator	80	string	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.

Attribute	AVP Type	Type	Description
Service-Type	6	enum	<p>Optional. The following settings are available:</p> <ul style="list-style-type: none"> - administrative—The user granted access to the administrative interface. - authenticate-only—Authentication is requested, and no authentication information needs to be returned. - call-check—This setting is used by the NAS in an Access-Request packet or Access-Accept packet to answer the call. - callback-administrative—The user disconnected, called back, and granted access to the administrative interface. - callback-framed—The user disconnected and called back and then used a Framed-Protocol attribute. - callback-login—The user disconnected and called back. - callback-nas-prompt—The user disconnected and called back and then provided a command prompt. - framed—The user used a Framed-Protocol attribute. - login—The user should be connected to a host. - nas-prompt—The user provided a command prompt on the NAS. - none—Disable the Service-Type AVP. - outbound—The user granted access to outgoing devices. <p>The default is <code>none</code> for 802.1x authentication. MAC Authentication Bypass (MAB) always uses the <code>call-check</code> setting, no matter what is configured.</p>

Attributes sent from the RADIUS server to the FortiSwitch unit during 802.1x authentication (Access-Accept)

Attribute	AVP Type	Type	Description
User-Name	1	alphanumeric	User name of supplicant (MAC address of host in MAB)
Class	25	string	Whatever the server returns
Tunnel-Type	64	enum	Optional. Set to 13 for VLAN.
Tunnel-Medium-Type	65	vsa	Optional. Set to 6 for IEEE-802.
Tunnel-Private-Group-ID	81	text	VLAN number or VLAN name
Vendor-Specific	26	vsa	Fortinet-Group-Name
Filter-Id	11	text	Relayed from the server
Session-Timeout	27	integer	How many seconds before the session times out

RADIUS attributes in the Accounting Start message

Attribute	AVP Type	Description
Acct-Status-Type	40	1 for Start
Acct-Session-Id	44	802.1x or MAB session ID generated by the switch. For example: 0000004b
User-Name	1	Host login name or MAC address. For example: host01
Acct-Multi-Session-Id	50	For example, e81cba8e8146 in MAC mode. This attribute cannot be used in port mode. The minimum value is 1; the maximum value is 1.
NAS-Identifier	32	For example, S148EP591900009 for the host name of the switch.
Framed-IP-Address	8	This value is the host IP address if is found in the switch; otherwise, the switch does not send this attribute. For example: 100.1.0.3
NAS-Port-Id	87	This value is a text string that identifies the port of the NAS connected to the host. For example: port48
NAS-Port	5	This value indicates the physical port number of the NAS. For example: 48
NAS-Port-Type	61	0 for asynchronous
Called-Station-Id	30	MAC address of the 802.1x port. For example: E8-1C-BA-8E-81-46
Calling-Station-Id	31	MAC address of host. For example: 00-12-01-00-00-01
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Filter-Id	11	Relayed from the server
Vendor-Specific	26	Fortinet-Group-Name. Authentication fails if this value does not match.
Class	25	Whatever the server returns

RADIUS attributes in the Accounting Interim Update message

Attribute	AVP Type	Description
Acct-Status-Type	40	3 for Interim-Update
Acct-Session-Id	44	802.1x or MAB session ID generated by the switch. For example: 0000004b
User-Name	1	Host login name or MAC address. For example: host01

Attribute	AVP Type	Description
Acct-Multi-Session-Id	50	For example, e81cba8e8146 in MAC mode. This attribute cannot be used in port mode.
Acct-Link-Count	51	2 for two sessions on the port. This attribute is only valid for MAC mode.
NAS-Identifier	32	For example, S148EP591900009 for the host name of the switch.
Framed-IP-Address	8	This value is the host IP address if it is found in the switch; otherwise, the switch does not send this attribute. For example: 100.1.0.3
NAS-Port-Id	87	This value is a text string that identifies the port of the NAS connected to the host. For example: port48
NAS-Port	5	This value indicates the physical port number of the NAS. For example: 48
NAS-Port-Type	61	15 for Ethernet
Called-Station-Id	30	MAC address of the 802.1x port. For example: E8-1C-BA-8E-81-46
Calling-Station-Id	31	MAC address of host. For example: 00-12-01-00-00-01
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Filter-Id	11	Eng-Group. If Filter-Id is received during authentication, it is included in accounting.
Class	25	Whatever the server returns
Vendor-Specific	26	Fortinet-Group-Name. Authentication fails if this value does not match.

RADIUS attributes in the Accounting Stop message

Attribute	AVP Type	Description
Acct-Status-Type	40	2 for Stop
Acct-Session-Id	44	802.1x or MAB session ID generated by the switch. For example: 0000004b
User-Name	1	Host login name or MAC address. For example: host01
Acct-Multi-Session-Id	50	For example, e81cba8e8146 in MAC mode. This attribute cannot be used in port mode.

Attribute	AVP Type	Description
Acct-Link-Count	51	2 for two sessions on the port
NAS-Identifier	32	For example, S148EP591900009 for the host name of the switch.
Framed-IP-Address	8	This value is the host IP address if it is found in the switch; otherwise, the switch does not send this attribute. For example: 100.1.0.3
NAS-Port-Id	87	This value is a text string that identifies the port of the NAS connected to the host. For example: port48
NAS-Port	5	This value indicates the physical port number of the NAS. For example: 48
NAS-Port-Type	61	15 for Ethernet
Called-Station-Id	30	MAC address of the 802.1x port. For example: E8-1C-BA-8E-81-46
Calling-Station-Id	31	MAC address of host. For example: 00-12-01-00-00-01
Acct-Input-Octets	42	3200
Acct-Output-Octets	43	16050448
Acct-Input-Packets	47	20
Acct-Output-Packets	48	93606
Acct-Terminate-Cause	49	6 for Admin-Reset
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Filter-Id	11	Eng-Group. If Filter-Id is received during authentication, it is included in accounting.
Class	25	Whatever the server returns
Vendor-Specific	26	Fortinet-Group-Name. Authentication fails if this value does not match.

RADIUS attributes in the Disconnect-Request message

Attribute	AVP Type	Description
Calling-Station-ID	31	MAC address of host
Framed-IP-Address	8	IP address of host

Attribute	AVP Type	Description
User-Name	1	Host login name
NAS-IP-Address	4	NAS IP address
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time

RADIUS attributes in the Disconnect-ACK message

Attribute	AVP Type	Description
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.

RADIUS attributes in the Disconnect-NAK message

Attribute	AVP Type	Description
Calling-Station-ID	31	MAC address of host
NAS-Port	5	Port that the host is connected to
Acct-Session-Id	44	802.1x or MAB session identifier generated by the switch
Framed-IP-Address	8	IP address of host
User-Name	1	Host login name
Error-Cause	101	Refer to the "Error-Cause codes in RADIUS CoA-NAK and Disconnect-NAK messages" table in this appendix for a listing of error causes, error codes, and descriptions.

RADIUS attributes in the CoA-Request message (reauth-port)

Attribute	AVP Type	Description
Calling-Station-ID	31	MAC address of host
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.
Vendor-Specific	26	Fortinet-Group-Name
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
User-Name	1	Host login name

RADIUS attributes in the CoA-Request message (disable-port)

Attribute	AVP Type	Description
Calling-Station-ID	31	MAC address of host
User-Name	1	Host login name
NAS-IP-Address	4	NAS IP address
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.
Vendor-Specific	26	Fortinet-Group-Name
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Class	25	Whatever the server returns
Filter-Id	11	Relayed from the server

RADIUS attributes in the CoA-Request message (bounce-port)

Attribute	AVP Type	Description
Calling-Station-ID	31	MAC address of host

Attribute	AVP Type	Description
User-Name	1	Host login name
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.
Vendor-Specific	26	Fortinet-Group-Name
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Class	25	Whatever the server returns
Filter-Id	11	Relayed from the server

RADIUS attributes in the CoA-Request message (session-timeout)

Attribute	AVP Type	Description
Calling-Station-ID	31	MAC address of host
NAS-Port	5	Port that the host is connected to
Acct-Session-Id	44	802.1x or MAB session identifier generated by the switch
Framed-IP-Address	8	IP address of host
User-Name	1	Host login name

RADIUS attributes in the CoA-ACK message

Attribute	AVP Type	Description
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.

RADIUS attributes in the CoA-NAK message

Attribute	AVP Type	Description
Error-Cause	101	Refer to the “Error-Cause codes in RADIUS CoA-NAK and Disconnect-NAK messages” table in this appendix for a listing of error causes, error codes, and descriptions.
Event-Timestamp	55	Time when the event occurred. For example: May 31, 2019 12:25:03.00000000 Pacific Daylight Time
Message-Authenticator	80	The Message-Authenticator attribute is a checksum of the entire Access-Request packet, containing the Type, ID, Length, and Authenticator field; the shared secret is used as the key.

Error-Cause codes in RADIUS CoA-NAK and Disconnect-NAK messages

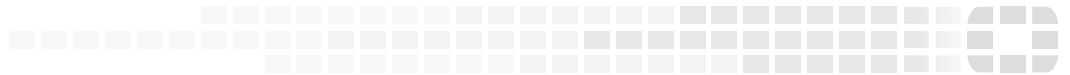
Error Cause	Error Code	Description
Unsupported Attribute	401	This error is a fatal error, which is sent if a request contains an attribute that is not supported.
NAS Identification Mismatch	403	This error is a fatal error, which is sent if one or more NAS-Identifier Attributes do not match the identity of the NAS receiving the request.
Invalid Attribute Value	407	This error is a fatal error, which is sent if a CoA-Request or Disconnect-Request message contains an attribute with an unsupported value.
Session Context Not Found	503	This error is a fatal error if the session context identified in the CoA-Request or Disconnect-Request message does not exist on the NAS.

Stop error codes for RADIUS accounting

Error Message	Error Code	Description
ACCT_TERM_CAUSE_IDLE_TIMEOUT	4	The system has been idle for too long.
ACCT_TERM_CAUSE_USER_REQUEST	1	The user requested the service to be stopped.
ACCT_TERM_CAUSE_SESSION_TIMEOUT	5	The session has timed out.
ACCT_TERM_CAUSE_ADMIN_RESET	6	The administrator has reset the session or port.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.