



FortiSwitchOS 3.x Administration Guide

Standalone Mode

Version 3.3.x

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

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

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



Monday, October 12, 2015

FortiSwitchOS-3.3.x Administration Guide Standalone Mode

TABLE OF CONTENTS

Change Log	7
Introduction	8
Supported Models.....	8
Supported Features: Release 3.0.0.....	8
Supported Features: Release 3.0.1.....	8
Supported Features: Release 3.2.0.....	9
Supported Features: Release 3.3.....	10
FortiSwitch 100.....	10
FortiSwitch 200.....	11
FortiSwitch 400.....	12
FortiSwitch 500.....	13
FortiSwitch 1000.....	14
FortiSwitch 3000.....	15
Before You Begin.....	16
How this Guide is Organized.....	16
System Settings	17
IP Conflict Detection.....	17
Description.....	17
Configuring IP Conflict Detection.....	17
Viewing IP Conflict Detection.....	17
Port Flap Guard.....	17
Configuring Port Flap Guard.....	18
Viewing Port Flap Guard Configuration.....	18
Management Ports	19
Models without Dedicated Management Port.....	19
Models with Dedicated Management Port.....	20
Remote Access to Management Port.....	20
Example Configurations.....	21
Physical Port Settings	26
Diagnostic Monitoring Interface (DMI) Module Status.....	26
Auto-Module Speed Detection.....	27
Enabling Auto-Module speed detection on a Port.....	27
Viewing Auto-Module Configuration.....	27
Link-Layer Discovery Protocol.....	27

Enabling LLDP on a Port	28
Viewing LLDP Configuration	28
Power over Ethernet	28
Enabling PoE on a Port	28
Determining the PoE Power Capacity	28
Reset the PoE Power on a Port	29
Display PoE information for a Port	29
Spanning Tree Protocol	30
MSTP Overview and terminology	30
Regions	30
IST	30
CST	30
Hop Count and Message Age	30
MSTP configuration	31
Configuring STP settings	31
Configuring an MST instance	32
Interactions outside of the MSTP Region	34
Example Configuration	34
Viewing the MSTP Configuration	34
VLAN Tagging	35
Native VLAN	35
Allowed VLAN List	35
Packet Processing	36
Ingress Port	36
Egress Port	36
Example 1	37
Purple flow:	37
Blue flow:	37
Example 2	38
Green flow:	38
Blue flow:	38
Layer 2 Interfaces	39
Configuring Switched Interfaces	39
Viewing Interface Configuration	39
Fortinet Loop Guard	39
Configuring Loop Guard	40
Viewing Loop Guard Configuration	40
Link Aggregation Groups	41
Configuring the Trunk and LAG Ports	41
Example Configuration	41
Viewing the Configured Trunk	43
Access Control Lists	44

Storm Control	48
Configuring Storm Control.....	48
IGMP Snooping	49
About IGMP Snooping.....	49
Limitations.....	49
Configuring IGMP Snooping.....	49
sFlow	53
About sFlow.....	53
Configuring sFlow.....	53
Port Mirroring	55
Configuring a Port Mirror.....	55
Multiple Mirror Destination Ports (MTP).....	55
Private VLANs	58
About Private VLANs.....	58
Private VLAN Example.....	58
Configuring SNMP Access.....	59
Layer 3 Interfaces	60
Switched Virtual Interfaces.....	60
Configuring a Switched Virtual Interface.....	60
Example SVI Configuration.....	60
Viewing SVI Configuration.....	61
Routed Interfaces.....	61
Configuring a Routed Interface.....	62
Example Routed Port Configuration.....	62
Viewing Routed Port Configuration.....	63
Layer 3 Routing in Hardware.....	63
Equal Cost Multi-Path (ECMP) Routing.....	64
Configuring ECMP.....	64
Example ECMP Configuration.....	64
Viewing ECMP Configuration.....	66
Bidirectional Forwarding Detection.....	66
Configuring BFD.....	66
Viewing BFD Configuration.....	67
IP-MAC Binding.....	67
Configuring IP-MAC Binding.....	67
Viewing IP-MAC Binding Configuration.....	68
802.1x Authentication	69
About 802.1x.....	69
Authenticating a Remote Admin with RADIUS.....	69
Authenticating with a RADIUS server.....	70
Example Configuration.....	71

TACACS	72
Administrative Accounts.....	72
Configuring an Access Profile for Admin Accounts.....	72
Configuring a TACACS Admin Account.....	72
User Accounts.....	73
Configuring a User Account.....	73
Configuring a User Group.....	73
Example Configuration.....	73
Troubleshooting and Support	75
TFTP Network Port.....	75
Set the Boot Partition.....	75

Change Log

Date	Change Description
Oct 24, 2014	Added content for initial 3.0.0 release.
Nov 21, 2014	Added chapter to describe Private VLANs.
Dec 4, 2014	Added content for release 3.0.1
Feb 17, 2015	Added content for release 3.2.0
Mar 6, 2015	Added new chapter for MSTP
Mar 25, 2015	Added MSTP diagnostic commands. Added chapter to describe VLAN Tagging.
July 22, 2015	Added features for FortiSwitchOS 3.3.0 release.
Aug 4, 2015	Added POE diagnostic command. Removed specific model numbers from POE description. Added note that auto-speed detection is supported for 1/10G ports but not 40G ports. Changed DMI note to indicate that DMI is supported on all models except 124D.
Aug 20, 2015	Minor update for release 3.3.1. Software Routing supported on some switch models.
Sept 18, 2015	New switch models released: FS-248D-FPOE and FS-524D-FPOE In Troubleshooting, added the command to set the boot partition.
Sept 23, 2015	New switch model released: FS-424D-FPOE
Oct 6, 2015	New switch models released: FS-548D and FS-524D

Introduction

This guide provides information about configuring a FortiSwitch unit in standalone mode. In standalone mode, you manage the FortiSwitch 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 using a FortiGate unit, please see the following guide: [Managing a FortiSwitch with a FortiGate](#).

Supported Models

This guide is for all FortiSwitch models that are supported by FortiSwitchOS. This includes the following models: FS-108D-POE, FS-124D, FS-124D-POE, FS-224D-POE, FS-224D-FPOE, FS-248D-FPOE, FS-424D-FPOE, FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE, FS-1024D, FS-1048D, and FS-3032D.

FortiSwitch Rugged model FSR-112D-POE is also supported.

Supported Features: Release 3.0.0

Release 3.0.0 includes the following new switch features, which are available on all of the FortiSwitchOS models:

- CLI bios upgrade
- CPU-based static routing
- DMI module reading (for select modules)
- Fan/Temp/PSU monitoring
- Multi-port mirroring

In addition, FS-1024D, FS-1048D, and FS-3032D support Link Aggregation Groups with up to 24 ports.

Supported Features: Release 3.0.1

The following enhancements are included in FortiSwitchOS v3.0.1:

- Support FS-224D-POE FortiLink remote management mode (see Release Notes for supported FortiGate models).
- Added delay internals between PoE ports when they are enabled during bootup.

Supported Features: Release 3.2.0

Release 3.2.0 supports FortiLink remote management mode for FS-108D-POE, FSR-112D-POE, and FS-224D-POE (see Release Notes for supported FortiGate models).

The following table lists the new switch features in Release 3.2.0 and the switch models that support them.

Feature	FS-108D-POE FSR-112D-POE FS-224D-POE	FS-1024D	FS-1048D	FS-3032D
Multi-port mirroring	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓
Flap guard	✓	✓	✓	✓
LAG min-max bundle	✓	✓	✓	✓
Auto-module max speed detection		✓	✓	
IP conflict detection and notification	✓	✓	✓	✓
Layer 3 routing in hardware		✓	✓	✓
Hardware-based ECMP		✓	✓	✓
MAC-IP Binding		✓	✓	✓
Static BFD		✓	✓	✓
48 port LAG support			✓	

Supported Features: Release 3.3

The following tables list the switch features in Release 3.3 that are supported on the 100, 200, 400, 500, 1000 and 3000 series of switch models. All features are available starting in release 3.3.0, unless otherwise noted.

FortiSwitch 100

Feature	FWS-108D-POE	FWS-R-112D-FPOE	FWS-124D	FWS-124D-POE
802.1x MAC base security mode	✓	✓	✓	✓
48 port lag support				
Auto module max speed detection & notification				
IP conflict detection & notification	✓	✓	✓	✓
MAC-IP Binding				
Static BFD				
HW based ECMP				
LLDP transmit	✓	✓	✓	✓
Loop-guard	✓	✓	✓	✓
LAG min-max-bundle	✓	✓	✓	✓
SFLOW, Storm Control	✓	✓	✓	✓
ACL, IGMP Snooping			✓	✓
Static L3/HW based routing				
Software Routing Only	✓	✓	✓	✓
CPLD Software Upgrade Support for OS				

FortiSwitch 200

Feature	F5W-224D-POE	F5W-224D-FPOE	F5W-248D-FPOE
802.1x MAC base security mode	✓	✓	✓
48 port lag support			✓
Auto module max speed detection & notification			
IP conflict detection & notification	✓	✓	✓
MAC-IP Binding			
Static BFD			
HW based ECMP			
LLDP transmit	✓	✓	✓
Loop-guard	✓	✓	✓
LAG min-max-bundle	✓	✓	✓
SFLOW, Storm Control	✓	✓	✓
ACL, IGMP Snooping		✓	✓
Static L3/HW based routing			
Software Routing Only	✓	✓	✓
CPLD Software Upgrade Support for OS			

FortiSwitch 400

Feature	FSW-424D-FPOE
802.1x MAC base security mode	✓
48 port lag support	
Auto module max speed detection & notification	✓
IP conflict detection & notification	✓
MAC-IP Binding	
Static BFD	
HW based ECMP	
LLDP transmit	✓
Loop-guard	✓
LAG min-max-bundle	✓
SFLOW, Storm Control	✓
ACL, IGMP Snooping	✓
Static L3/HW based routing	
Software Routing Only	✓
CPLD Software Upgrade Support for OS	

FortiSwitch 500

Feature	FSW-524D	FSW-524D-FPOE	FSW-548D	FSW-548D-FPOE
802.1x MAC base security mode	✓	✓	✓	✓
48 port lag support			✓	✓
Auto module max speed detection & notification	✓	✓	✓	✓
IP conflict detection & notification	✓	✓	✓	✓
MAC-IP Binding				
Static BFD				
HW based ECMP	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓
Loop-guard	✓	✓	✓	✓
LAG min-max-bundle	✓	✓	✓	✓
SFLOW, Storm Control	✓	✓	✓	✓
ACL, IGMP Snooping	✓	✓	✓	✓
Static L3/HW based routing	✓	✓	✓	✓
Software Routing Only				
CPLD Software Upgrade Support for OS				

FortiSwitch 1000

Feature	F5W-1024D	F5W-1048D
802.1x MAC base security mode	✓	✓
48 port lag support		✓
Auto module max speed detection & notification	✓	✓
IP conflict detection & notification	✓	✓
MAC-IP Binding	✓	✓
Static BFD	✓	✓
HW based ECMP	✓	✓
LLDP transmit	✓	✓
Loop-guard	✓	✓
LAG min-max-bundle	✓	✓
SFLOW, Storm Control	✓	✓
ACL, IGMP Snooping	✓	✓
Static L3/HW based routing	✓	✓
Software Routing Only		
CPLD Software Upgrade Support for OS (release 3.3.1)	✓	✓

FortiSwitch 3000

Feature	F5W-3032D
802.1x MAC base security mode	✓
48 port lag support	
Auto module max speed detection & notification	
IP conflict detection & notification	✓
MAC-IP Binding	✓
Static BFD	✓
HW based ECMP	✓
LLDP transmit	✓
Loop-guard	✓
LAG min-max-bundle	✓
SFLOW, Storm Control	✓
ACL, IGMP Snooping	✓
Static L3/HW based routing	✓
Software Routing Only	
CPLD Software Upgrade Support for OS	

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 web-based manager and CLI.

How this Guide is Organized

This guide is organized into the following chapters:

- [System Settings](#) - the initial configuration of your FortiSwitch unit.
- [Management Ports](#) - configuring the management ports.
- [Physical Port Settings](#) - configuring the physical ports.
- [Spanning Tree Protocol](#) - how to configure MSTP.
- [VLAN Tagging](#) - configuration and packet flow for VLAN-tagged and untagged packets.
- [Layer 2 Interfaces](#) - configuring Layer 2 interfaces.
- [Link Aggregation Groups](#) - configuring Link Aggregation Groups.
- [Access Control Lists](#) - configuring ACLs
- [Storm Control](#) - configuring Storm Control
- [IGMP Snooping](#) - configuring IGMP Snooping
- [sFlow](#) - configuring sFlow.
- [Port Mirroring](#) - configuring Port Mirroring.
- [Private VLANs](#) - creation and management of private virtual local area networks (VLANs).
- [Layer 3 Interfaces](#) - configuring routed ports, routed VLAN interfaces, switch virtual interfaces, and features related to these interfaces.
- [802.1x Authentication](#) - configuring 802.1x authentication.
- [TACACS](#) - configuring TACACS authentication.

System Settings

IP Conflict Detection

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

Description

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 actively broadcasts gratuitous ARP packets when any of the following events occurs:

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

If a system is using the same IP address, the FortiSwitch will receive 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 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 can create instability in protocols such as STP. If a port is flapping, STP must continually recalculate the role for each port.

The port flap guard feature will detect a flapping port and the system will shut down the port if necessary. You can manually reset the port and restore it to the enabled state.

Configuring Port Flap Guard

Port flap-guard is configured and enabled on a global basis. The default setting is disabled.

Flap duration range is 5 to 300

Flap rate range is 5 to 300

Using the CLI:

```
config switch flapguard settings
  set status [ disable | enable ]
  set flap-rate <integer>
  set flap-duration <integer>
```

Use the following command to reset a port and restore it to service:

```
execute flapguard reset <port>
```

Viewing Port Flap Guard Configuration

Display the status of Port Flap Guard configuration using following commands

```
show switch flapguard settings
```

Display the Port Flap Guard information for each port using the following command:

```
diagnose flapguard instance status
```

Management Ports

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

Models without 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 web-based manager:

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

1. Go to **System > Network > Interface** and edit the **internal** interface.
2. Assign an **IP/Netmask**.
3. Set **Administrative Access** to use the desired protocols to connect to the interface.
4. Select **OK**.

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

1. Go to **System > Network > Interface** and select **Create New** to create a management VLAN.
2. Give the interface an appropriate name.
3. Set **Interface** to **internal**.
4. Set a **VLAN ID**.
5. Assign an **IP/Netmask**.
6. Set **Administrative Access** to use the desired protocols to connect to the interface.
7. Select **OK**.

Using the CLI:

```
config system interface
  edit internal
    set ip <address>
    set allowaccess <access_types>
    set type physical
  next
  edit <vlan name>
    set ip <address>
    set allowaccess <access_types>
    set interface internal
    set vlanid <VLAN id>
  end
end
```

Models with 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 id of 4094.

Using the web-based manager:

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

1. Go to **System > Network > Interface** and edit the **mgmt** interface.
2. Assign an **IP/Netmask**.
3. Set **Administrative Access** to use the desired protocols to connect to the interface.
4. Select **OK**.

Using the CLI:

```
config system interface
  edit mgmt
    set ip <address>
    set allowaccess <access_types>
    set type physical
  next
  edit internal
    set type physical
  end
end
```

Remote Access to 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 CLI:

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

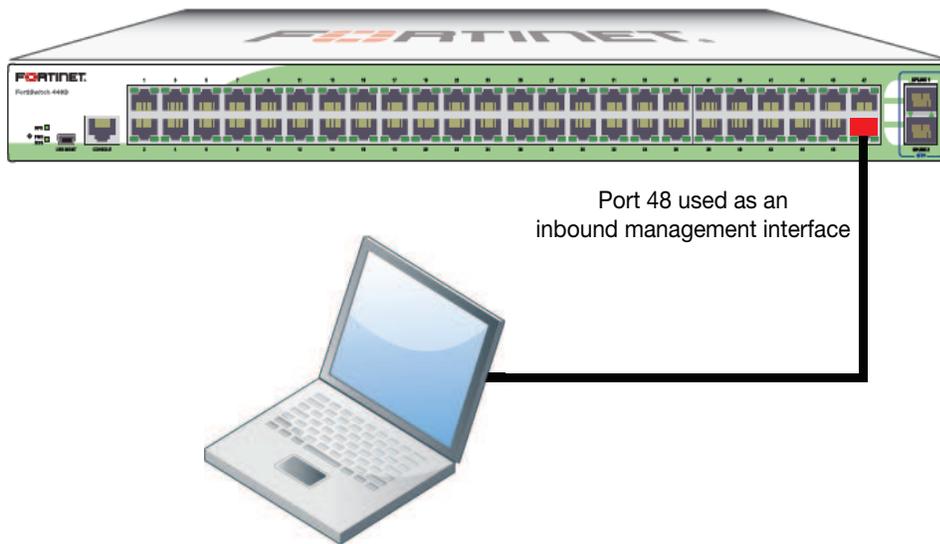
Example Configurations

The following are four example configurations for management ports, with the CLI syntax shown to create them.

Example 1: Port 48 as an inbound management interface

In this example, a physical port is used as an inbound management interface. Also, the FortiSwitch in the example has no default VLAN configured to connect its **internal** interface to any physical port.

Using Port 48 of a FortiSwitch-448B unit



Syntax

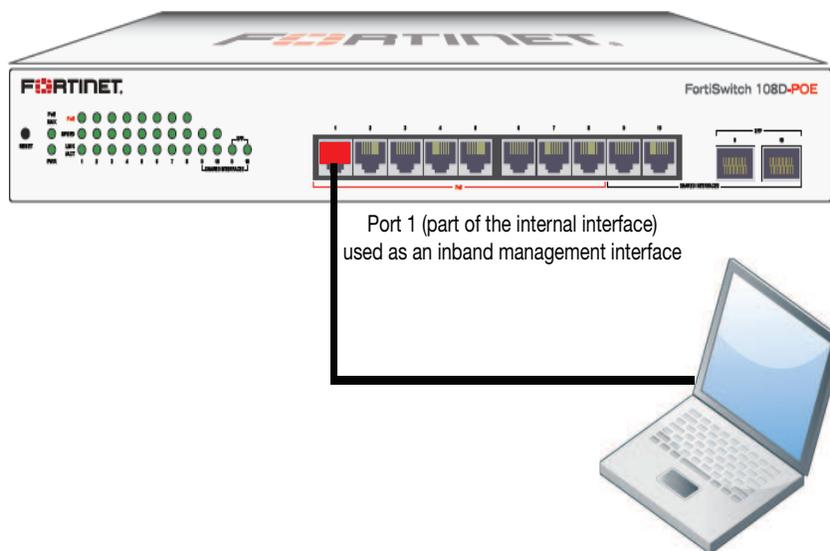
```
config system interface
  edit internal
    set type physical
  next
  edit mgmt-vlan
    set ip 10.105.142.22 255.255.255.0
    set allowaccess ping https ssh
    set interface "internal"
    set vlanid 4090
  next
end
config switch interface
  edit port48
    set native-vlan 4090
    set stp-state disabled
  next
  edit uplink1
  next
  edit uplink2
  next
```

```
edit internal
  set native-vlan 4095
  set allowed-vlans 4090
  set stp-state disabled
end
end
```

Example 2: Internal interface as an inbound management interface

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

Using the internal interface of a FortiSwitch-108D-POE



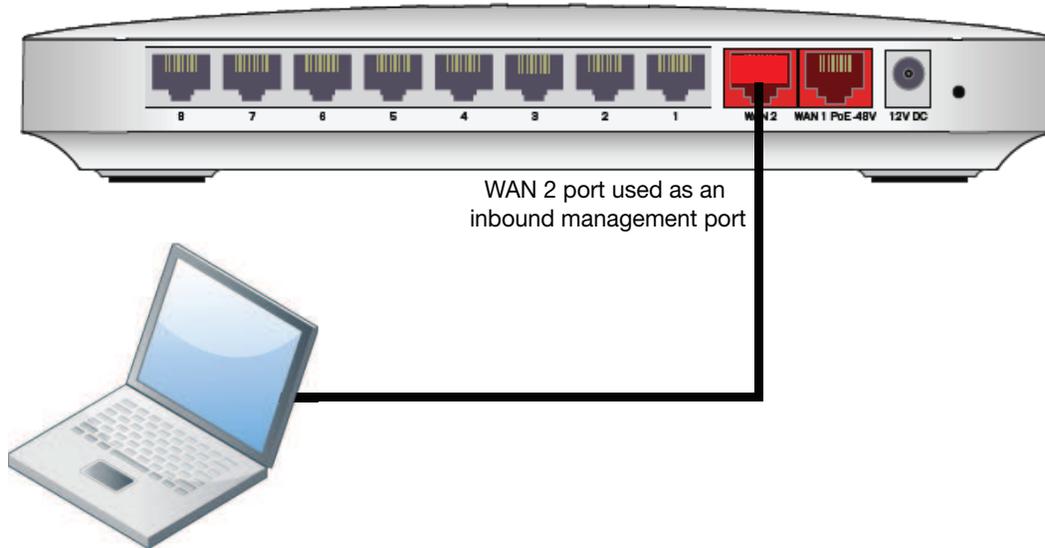
Syntax

```
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
```

Example 3: WAN interface as an inbound management port

In this example, the WAN interface is used as an inbound management port.

WAN interface of a FortiSwitch-28C



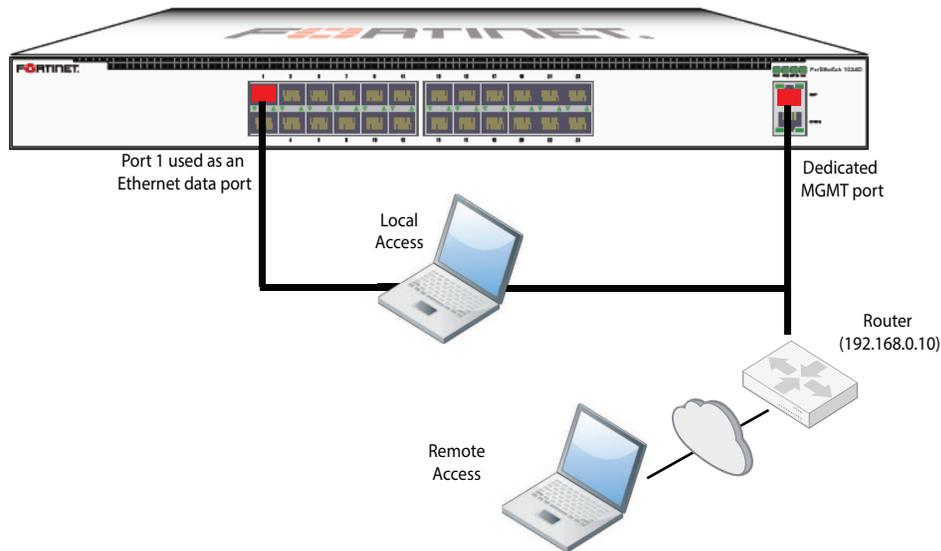
Syntax

```
config system interface
  edit wan2
    set ip 10.105.142.10 255.255.255.0
    set allowaccess ping https ssh
    set type physical
  next
  edit wan1
    set mode dhcp
    set allowaccess ping https ssh
    set type physical
    set defaultgw enable
  next
  edit internal
    set type physical
  end
end
```

Example 4: Out of band management interface

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

Out of band management on a FortiSwitch-1024D



Syntax

```
// option 1: management port with static IP

config system interface
  edit mgmt
    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
  end
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
end
```

Physical Port Settings

This chapter covers features that are associated with FortiSwitch physical ports.

Diagnostic Monitoring Interface (DMI) Module Status



DMI is supported on all models except FortiSwitch 124D.

DMI module status can be viewed using the command **get switch modules**. This allows you to display one of the following:

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

Below is an example output for the command switch modules detail:

```
Port (port38)
identifier      SFP/SFP+
connector      LC
transceiver    10G Base-SR
encoding       64B/66B
Length Decode Common
length_smf_1km N/A
length_cable   N/A
SFP Specific
length_smf_100m N/A
length_50um_om2 80 meter
length_62um_om1 30 meter
length_50um_om3 150 meter
vendor         FINISAR CORP.
vendor_oid     0x009065
vendor_pn      FTLX8572D3BCL
vendor_rev     A
vendor_sn      UDK050K
manuf_date     02/20/2009
```

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 there is a problem reading from the module, the system sets the default speed (the default value is platform-specific).

When auto-module sets the speed, the system creates a log entry noting the speed that was set.

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

Enabling Auto-Module speed detection on a Port

```
config switch physical-port
  edit <port>
    set speed auto-module
  end
end
```

Viewing Auto-Module Configuration

Display the status of Auto-Module using following command

```
FS # config switch physical-port
FS (physical-port) # edit port47
FS(port47) # show
  config switch physical-port
    edit "port47"
      set max-frame-size 16360
      set speed 10000full
    next
  end
FS(port47) # 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
```

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.

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

LLDP transmission is configured per port. By default LLDP transmission is disabled.

Enabling LLDP on a Port

```
config switch physical-port
  edit <port>
    set lldp-transmit [ enable | disable ]
  next
end
```

Viewing LLDP Configuration

Use the following command to display the LLDP errors:

```
get switch lldp errors

LLDP errors:
Total memory allocation failures: 0
Total unrecognized TLVs: 0
```

Use the following commands to display the LLDP information about the Layer 2 peers for a specified port:

```
get switch lldp (neighbors-summary | neighbors-detail) <port>
```

Power over Ethernet

This section contains information on using Power over Ethernet (PoE) with your FortiSwitch.



Power over Ethernet is only available on models with the POE suffix in the model number, such as FS-108D-POE.

Enabling PoE on a Port

```
config switch physical-port
  edit <port>
    set poe-status enable
  end
end
```

Determining the PoE Power Capacity

To determine the PoE power capacity, use the following command:

```
get switch poe inline
```

Reset the PoE Power on a Port

To reset the PoE power on a port, use the following command:

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

Display PoE information for a Port

To display PoE information for a port, use the following command:

```
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
```

Spanning Tree Protocol

Spanning tree protocol is a link-management protocol that ensures a loop-free Layer 2 network topology.

FortiSwitch supports the Multiple Spanning Tree Protocol (MSTP), which is defined in the IEEE 802.1Q standard.

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 RSTP. A given Layer 2 network may 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 MST configuration (region name, MST revision number and VLAN-to-instance mapping). A network may have any number of regions. Regions are independent of each other (VLAN-to-instance mapping is different in each region).

FortiSwitch 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 STP protocols.

IST

Instance 0 is a special instance, called the 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 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 hop count set to Maximum 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.

MSTP configuration

Configuration consist of two steps:

- configure STP settings that are common to all MST instances.
- configure settings that are specific to each MST instance.

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 web-based manager:

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

Settings	Guidelines
Enable	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. Range of values is 0 - 65535 Default value is 0.
Hello-Time	Hello time is how often (in seconds) that the switch sends out a BPDU. Range of values is 1 to 10. Default value is 2.
Forward-Time	Forward time is how long (in seconds) a port will spend in listening and learning state before transitioning to forwarding state. Range of values is 4 to 30. Default value is 15.

Settings	Guidelines
Max-Age	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. Range of values is 6 to 40. 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. Range of values is 1 to 40. Default value is 20.

Using the CLI:

```

config switch stp settings
  set forward-time <4 - 30>
  set hello-time <1 - 10>
  set max-age <6 - 40>
  set max-hops <1 - 40>
  set name <region name>
  set revision <0 - x>
  set status {enable | disable}
end

```

Configuring an MST instance

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 web-based manager:

1. Go to Switch > STP > Instance
2. Create a new MST instance, or select an existing instance to edit.
3. Update the instance parameters as described in the following table.
4. Click Apply to save the settings.

Settings	Guidelines
ID	Instance ID. Range is 1 - 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 Default value is 32768
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 PBDU root cost in any BPDU sent on this port. A lower value is preferred. The range of values is 1 to 200,000,000. 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. Default value : 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
```

Interactions outside of the MSTP Region

A boundary port on an MST switch is a port that receives an STP (version 0) BPDU or an RSTP (version 2) BPDU, or a PBDU 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, since the RSTP switch will read this as an RSTP BPDU.

Example Configuration

The following is an example CLI configuration:

<a simple example would be useful.>

Viewing the MSTP Configuration

In order 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
```

VLAN Tagging

FortiSwitch ports will 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 provides port parameters to configure and manage VLAN tagging.

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. The native VLAN is NOT an allowed value for an incoming tagged packet.

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

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 (which excludes the native VLAN)
- packet keeps the VLAN tag and is allowed to proceed

Egress Port

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

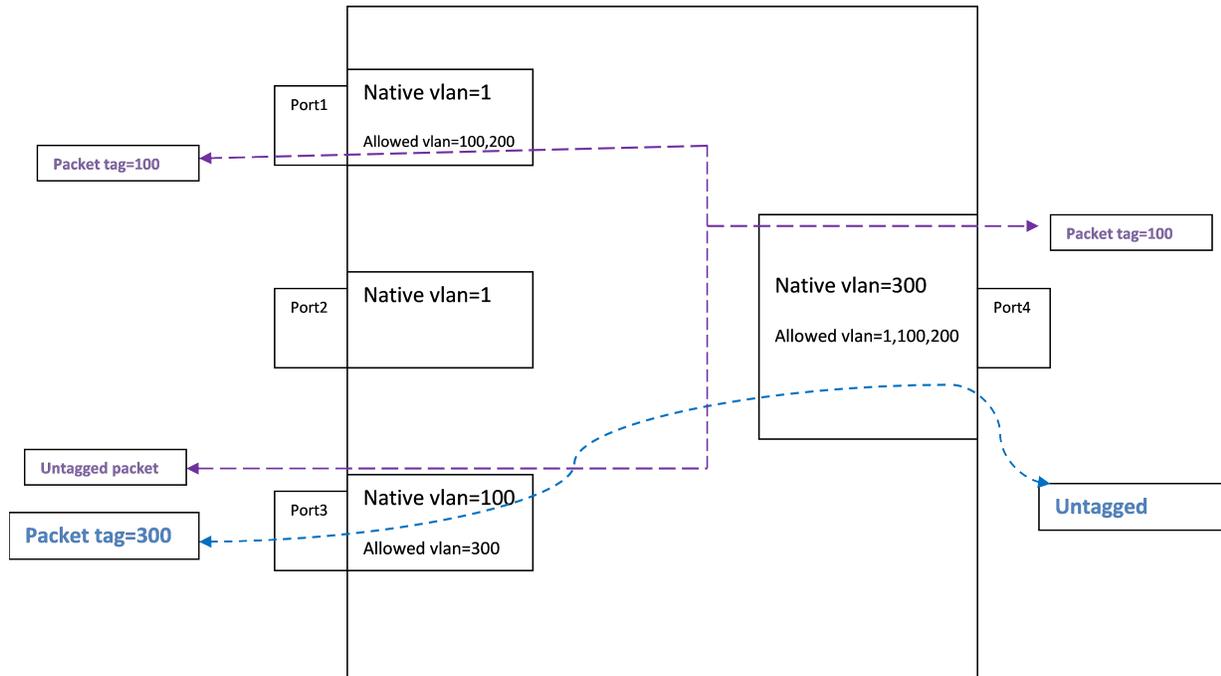
If the packet tag value is on the Allowed VLAN list, the packet is sent out with the existing tag.

if the packet tag value is the native VLAN, the tag is stripped and then the packet is sent out.

Otherwise the packet is dropped.

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.

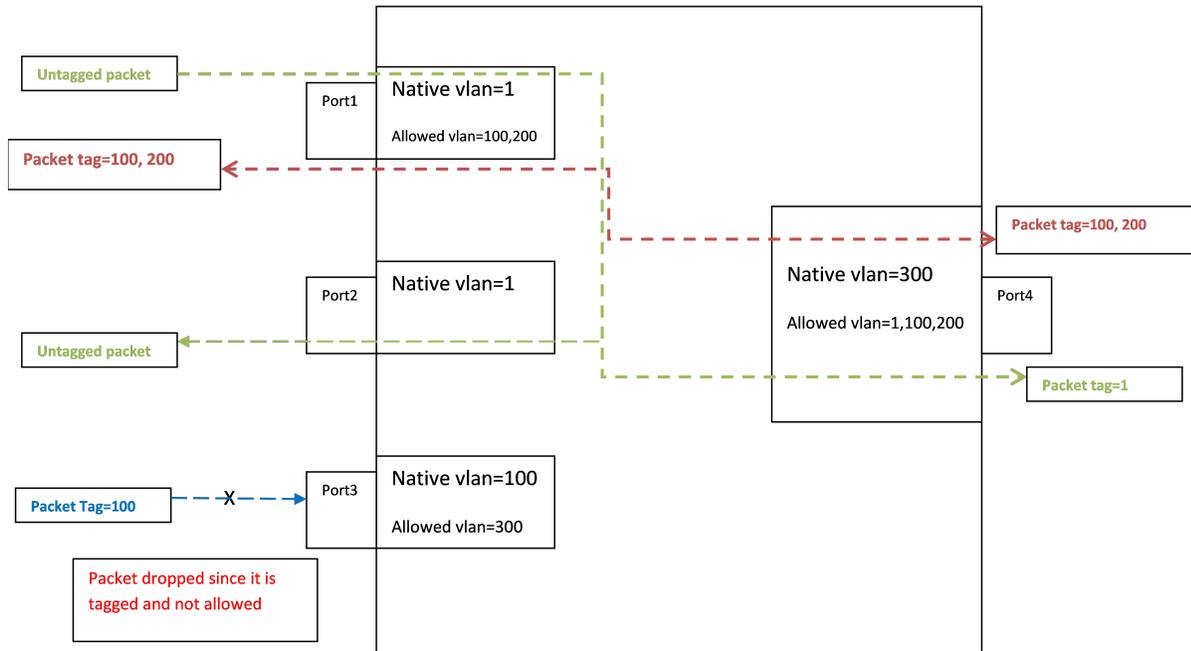
Blue flow:

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 not allowed, because 100 is the native VLAN.

Layer 2 Interfaces

This chapter provides information about configuring FortiSwitch layer 2 interfaces.

Configuring Switched Interfaces

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

You can configure optional capabilities such as Loop Guard, IEEE 802.1x authentication, and Private VLAN. These capabilities are covered in subsequent sections of this document.

Using the web-based manager:

1. Go to **Switch > Interface > Interface**
2. Select one or more ports to update and click **Edit**.
3. If you selected more than one port, the port names are displayed in the name field, separated by commas.
4. Enter new values as required for Native VLAN, Allowed VLAN, Enable STP, Enable Edge Port, and Security Mode.
5. Click **OK** to save the changes.

Using the CLI:

```
config switch interface
  edit <port>
  set native-vlan <vlan>
  set allowed-vlans <vlan> [<vlan>] [<vlan> - <vlan>]
  set stp-state {enabled | disabled}
  set edge-port {enabled | disabled}
  set security-mode {none| dot1x}
```

Viewing Interface Configuration

Display port configuration using following command:

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

Display port settings using following command:

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

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. If a port detects a loop, the system takes the port out of service to protect the overall network.

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 sent out on a port is subsequently received by the same port, a loop exists downstream.

The system takes the port out of service. 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 CLI:

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

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

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

Viewing Loop Guard Configuration

Display the Loop Guard configuration for a port using following command:

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

Link Aggregation Groups

This chapter provides information on how to configure a Link Aggregation Group (LAG). For LAG control, FortiSwitch supports the industry-standard Link Aggregation Control Protocol (LACP).

FortiSwitch supports LACP protocol in active and passive modes.

In active mode, you can optionally specify the minimum and maximum number of active members in a trunk group.

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

Configuring the Trunk and LAG Ports



It is important to configure the trunk to prevent loops.

Using the web-based manager:

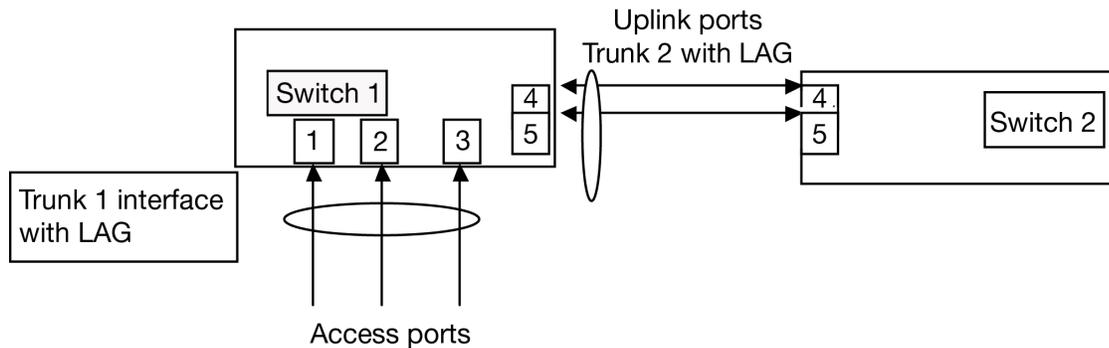
1. Go to **Switch > Port > Trunk** and select **Create Trunk**.
2. Give the trunk an appropriate name.
3. Set **Mode** to either **static**, **lACP-active** or **lACP-passive**.
4. Add the required ports to the **Members** list.
5. Select **OK**.

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-behaviour {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
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 port 1
    set native-vlan 1
  next
  edit port 2
    set native-vlan 2
  next
  edit port 3
    set native-vlan 3
  next
  edit port 4
    set native-vlan 4
    set allowed vlans 1 2 3
  next
  edit port 5
    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
```

Viewing the Configured Trunk

In order to see the details of a configured trunk, use the following command:

```
diagnose switch trunk list
```

Access Control Lists

You can use Access Control Lists (ACLs) to configure policies for different types of traffic.

Key attributes of a policy include:

1. **Interface.** The interface(s) on which traffic arrives at the switch (ingress) or leaves the switch (egress). The interface can be a port, a trunk, or all interfaces. A policy can apply to either ingress OR egress traffic
2. **Classifier.** The classifier identifies the packets that the policy will act on. Each packet can be classified based on a one or more criteria. Criteria include source and destination MAC address, VLAN id, source and destination IP address, service (layer 4 protocol id and port number), or schedule (day and/or time of day).
3. **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.
 - mark the packet

Major steps to configure an ACL include the following:

1. Create or customize a service. FortiSwitch provides a set of pre-configured services that you can use. Use the following command to list the services:


```
show switch acl service custom
```
2. (Optional) Create a policer, if you are defining ACLs to police different types of traffic.
3. Configure addresses. An address is a set of one or more IP addresses, an IP address and a subnet mask, or an IP address range. Each address must have a unique name
4. (Optional) Configure a schedule, if your ACL definition requires activation based on day or time of day.
5. Configure the security policies

The switch uses specialized TCAM memory to perform ACL matching. Each model of FortiSwitch provides different ACL-related capabilities. When you configure the ACL policy, the system will reject the request if the hardware cannot support it.

<http://docs.fortinet.com/d/fortigate-fortios-5.2-cli-reference>

1. Create or customize a service

```
config switch acl service custom
  edit <service name>
    set comment <string>
    set color
    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
end
```

2. Create a policer

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

Each policy is assigned a unique Universally Unique IDentifier (UUID) that is automatically assigned. To view it, use the command **get switch acl policy**.

3. Configure the policy

```
config switch acl policy
  edit <policy-id>
    set description
    set ingress-interface < port >
    set ingress-interface-all {enable | disable}
    config <classifier>
      set src-mac <mac> <mask>
      set dst-mac <mac> <mask>
      set ether-type <integer>
      set src-ip-prefix <IP address> <mask>
      set dest-ip-prefix <IP address> <mask>
      set service <service-id>
      set vlanid <vlan-id>
    end
    config action
      set count {enable | disable}
      set drop {enable | disable}
      set mirror [internal | <port>]
      set policer <policer>
      set redirect [internal | <port>]
    end
  end
```

Example 1

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

```
config switch acl service custom
  edit "SMB"
    set tcp-portrange 445
  next
end
config switch acl policy # apply policy to port 1 ingress and send to port 3
  edit 1
    set description "cnt_n_mirror_smb"
    set ingress-interface "port1"
    config action
      set count enable
      set mirror "port3"
    end
```

```
    config classifier
      set service "SMB"
      set src-ip-prefix 20.20.20.100 255.255.255.255
      set dst-ip-prefix 100.100.100.0 255.255.255.0
    end
  next
end
```

Example 2

FortiSwitch 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 FDDOS service profiles to different types of traffic.

```
config switch acl policy # 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 'Red'
  end
  set description "cnt_n_mirror13"
  set ingress-interface "port1"
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 'Red'
  end
  set description "cnt_n_mirror31"
  set ingress-interface "port3"
next
end

config switch acl policy # 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 'Yellow'
  end
  set description "cnt_n_mirror14"
  set ingress-interface "port1"
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 'Yellow'
    end
    set description "cnt_n_mirror41"
    set ingress-interface "port4"
next
end
```

Get commands

Use the following command to display the counters associated with a policy. If you do not provide a policy id, the system displays all policies that have counters.

```
get switch acl counters [policy-id]
ID Packets Bytes description
-----
0001 1861642 119145728 ip_mac_filter
0100 11160319 714260416 udp_vlan_filter
```

Execute commands

Use the following command to clear the counters associated with a policy. If you do not provide a policy id, the system clears all of the ACL counters.

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

Storm Control

Storm Control protects a LAN from being disrupted by traffic storms, which can be caused by mistakes in network configuration or denial-of-service attacks. A traffic storm creates excessive traffic on the LAN and degrades network performance. A traffic storm may consist of broadcast, multicast, or unicast traffic.

When you enable the Storm Control feature on FortiSwitch, it measures the data rate for unknown unicast, unknown multicast, and broadcast traffic. You can enable/disable Storm Control for each of these traffic types individually. If the traffic rate for any of the traffic types exceeds the configured threshold, FortiSwitch drops the excess traffic. The data rate is measured in packets-per-second.

Storm Control configuration is global to the whole switch. By default, Storm Control is disabled.

Configuring Storm Control

Use the following commands to configure Storm Control.

Specify the rate as packets-per-second. If you set the rate to zero, the system drops all packets (for the enabled traffic types).

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

Get commands

Use the following command to display the storm-control configuration.

```
get switch storm-control
```

IGMP Snooping

FortiSwitch uses the information passed in IGMP messages to optimize the forwarding of multicast traffic.

About IGMP Snooping

IGMP Snooping allows the FortiSwitch 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. FortiSwitch 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. FortiSwitch is also compatible with IGMPv1 and IGMPv2.

Basic IGMP-Snooping operation

1. Host expresses interest in joining a multicast group. (Sends or responds to a join message)
2. FortiSwitch creates 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. FortiSwitch removes the entry when the last host leaves the group (or the entry ages out).

Limitations

1. You must enable the IGMP-snooping function, using CLI command **igmp-snooping enable**, before configuring a multicast router port interface.
2. If a port is configured as a multicast router port, you must delete the multicast router port configuration before changing the native VLAN.
3. Currently, IGMPv3 (source-specific) is not fully supported. FortiSwitchOS can identify the IGMPv3 query/report messages, but the multicast group creation and traffic replication is based on multicast group address and VLAN only (IGMPv2 operation).
4. The IGMP snooping entries are added based on multicast group MAC address.
5. A multicast router port needs to be configured with a native VLAN that has IGMP snooping enabled. If users want to have IGMP snooping enabled on more than one VLAN interface, you need to configure an additional multicast router port.
6. Up to 10 multicast router interfaces can be statically configured or dynamically learned
7. IGMP Snooping is not supported on trunk interfaces.

Configuring IGMP Snooping

Configuring IGMP Snooping consists of the following major steps:

1. Assign VLANs and enable IGMP Snooping on the interfaces
2. Configure IGMP Snooping on the VLANs

1. Enable IGMP Snooping on the Interfaces

The **set igmp-snooping** interface subcommand allows or disallows IGMP Snooping on the specified switch interface (default is disabled).

```
config switch interface
  edit port2
    set native-vlan <vlan-id>
    set igmp-snooping [ allowed | not-allowed ]
  next
end
```

Use the following command to clear the learned/configured multicast group from an interface:

```
execute clear switch igmp-snoop <intf-name> <group-ip>
```

2. Configure IGMP Snooping on the VLANs

The **set igmp-snooping** VLAN subcommand enables or disables IGMP Snooping on the specified VLAN interface (default is disabled).

The **set igmps-fast-leave** command enables or disables IGMP fast leave on the specified VLAN. Fast-Leave supports IGMPv2 hosts that cannot be explicitly tracked because of the host report-suppression mechanism of the IGMPv2 Protocol. When this feature is enabled, IGMP Snooping software assume that no more than one host is present on each VLAN port. The default is disabled.

The **set igmps-report-suppression** command limits the membership report send to a multicast-capable router. The default is enabled.

The **set igmps-mcast-router-intf** command configures a static connection to a multicast router. The interface to the router must be in the specified VLAN. Note: currently, the system supports only one multicast router interface per vlan.

```
config switch vlan
  edit <vlan-id>
    set igmp-snooping [enable |disable]
    set igmps-fast-leave [enable |disable]
    set igmps-report-suppression [enable|disable]
    set igmps-mcast-router-intf <LIST OF INTF>
```

Example:

```
config switch vlan
  edit 30
    set igmp-snooping enable
    set igmps-fast-leave enable
    set igmps-report-suppression enable
    set igmps-mcast-router-intf port10
  next
end
```

Configuration Example

Configure native VLAN on the interface ports and enable IGMP-snooping

```
config switch interface
  edit port10
    set native-vlan 30
    set igmp-snooping allowed
  next
  edit port2
    set native-vlan 30
    set igmp-snooping allowed
  next
  edit port4
    set native-vlan 30
    set igmp-snooping allowed
  next
  edit port6
    set native-vlan 30
    set igmp-snooping allowed
  next
  edit port8
    set native-vlan 30
    set igmp-snooping allowed
  next
end
```

Configure IGMP-snooping on the VLAN:

```
config switch vlan
  edit 30
    set igmp-snooping enable
    ??set igmps-mcast-router-intf port10
  end
```

Display Commands

List the detail status of IGMP Snooping enabled interfaces.

This command also displays the VLAN interface names, which you can use in other commands. The system creates VLAN interface names as <vlan+Bridge-name.VLAN-ID>. The default Bridge-name is 1. Therefore the interface name for VLAN 30 is vlan1.30

```
FS1D243Z13000023 # get switch igmp-snooping interface
Interface vlan1.30 (Index 4294967295)
IGMP Enabled, Active, Non-Querier, Version 2 (default)
IGMP interface has 0 group-record states
IGMP activity: 0 joins, 0 leaves
IGMP querying router is 0.0.0.0
...
Interface sp2 (Index 18) (Vlan 30)
IGMP Snooping is globally enabled
IGMP Snooping is enabled on this interface
IGMP Snooping fast-leave is enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
```

...

List the multicast routers:

Display the list of multicast routers on the interface – both learned and configured.

```
get switch igmp-snooping mrouter <VLAN-IF-NAME>
```

IGMP snooping statics

Display IGMP snooping statics for the given VLAN interface.

```
FS1D243Z13000023 # get switch igmp-snooping stats vlan1.30
IGMP Snooping statistics for vlan1.30
Interface: vlan1.30
Group: 224.2.3.4
Flags:
Uptime: 00:01:00
Group mode: Exclude
Last reporter: 10.30.0.10
Source list is empty
```

Learned multicast groups

```
FS1D243Z13000023 # get switch igmp-snooping group
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
224.2.3.4 sp2 00:03:38 00:00:42 10.30.0.10
224.2.3.5 sp2 00:03:17 00:01:02 10.30.0.10
```

sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that may impact performance and throughput. sFlow provides a means for exporting truncated packets, together with interface counters. FortiSwitch implements sFlow version 5.

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. The information sent is only a sampling of the data for minimal impact on network throughput and performance.

The sFlow Collector receives the datagrams, and provides real-time analysis and graphing to indicate where potential traffic issues are occurring. sFlow Collector software is available from a number of third party software vendors.

sFlow data captures a sampling of network traffic. The sampled packets and counter information, referred to as flow samples and counter samples respectively, are sent as sFlow datagrams to an sFlow collector. The collector is a central server running software that analyzes and reports on network traffic.

For sFlow, you first define a collector by specifying its IP address.

You can configure sFlow on FortiSwitch ports.

sFlow supports trunks and VLANs.

Configuring sFlow

Configuration consists of the following steps:

- enabling the sFlow Agent
- configuring sampling information on the interfaces

Configure sFlow Agents

Use the following commands to enable an sFlow Agent:

1. Set the IP address of the collector.
2. Set the collector port number. This value is set as the destination port number in sFlow UDP packets. The default value is 6343.

```
config system sflow
    set collector-ip <ip/hostname>
    set collector-port <port>
```

Configure the Interfaces

Use the following commands to configure sFlow on a port:

1. Enable sFlow on the port. By default, sFlow is disabled.
2. Set the sample rate. An average of one out of **count** packets is randomly sampled. The default value is 512, and the range of values is 0-99999.
3. Set the direction for capturing the traffic. sFlow can capture the ingress traffic (RX), the egress traffic (TX), or both. The default is both.
4. Set the polling interval. The interval defines how often the switch sends interface counters to the collector. The default value is 30, and the range of values is 1-255.

```
config switch interface
  edit <port>
    set sflow-sampler [enabled | disabled]
    set sample-rate <count>
    set sample-direction [rx | tx | both]
    set polling-interval <interval>
```

Get commands

Use the following command to display the sflow configuration.

```
get system sflow
```

Port Mirroring

This chapter contains information on how to configure layer 2 port mirroring.

Configuring a Port Mirror

Using the web-based manager:

1. Go to **Switch > Port > Mirror**.
2. Enter a name for the mirror.
3. Set the **Status Enable** check box to set the mirror to active.
4. Select a Destination Port.
5. Select available ports to be used for Ingress Monitoring and Egress Monitoring.
6. Enable the **Packet switching functionality when mirroring** option 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.

Using the CLI:

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

Multiple Mirror Destination Ports (MTP)

With some FortiSwitch models, you can configure multiple mirror destination ports. However, note 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.
- For switch models FS-1024D, FS-1048D, and FS--3032D:
 - You can configure a maximum of four mirror destination ports.
 - You can configure a maximum of four ingress/egress ports.
 - The same ingress/egress port can be mirrored to more than one destination port.
- For switch models FS-108D-POE and FS-224D-POE:
 - You can configure up to seven port mirrors, each with a different destination port.

- There is no limit on the number of ingress or egress ports.
- An ingress or egress port cannot be mirrored to more than one destination port.

The above restrictions apply to active port mirrors. If you try to activate an invalid port mirror configuration, the system will display the `Insufficient resources!!` error message.

The following example configuration is valid for FortiSwitch-3032D:

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

(The above configuration includes three ingress ports, one egress port, and four destination ports. The port3 ingress and egress ports are mirrored to multiple destinations).

The following example configuration is valid for FortiSwitch-224D-POE:

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

(The above configuration includes three ingress ports, three egress ports and four destination ports. Each ingress and egress port is mirrored to only one destination port).

Private VLANs

This chapter contains information on the creation and management of private virtual local area networks (VLANs).

About Private VLANs

A Private VLAN divides the original VLAN, now called the Primary VLAN, into sub-VLANs (Secondary VLANs), while keeping the existing IP subnet and layer 3 configuration. Unlike a regular VLAN, which is a single broadcast domain, private VLANs partitions one broadcast domain into multiple smaller broadcast subdomains.

After a Private VLAN is configured, the Primary VLAN is used to forward frames downstream to all Secondary VLANs.

There are two main types of Secondary VLAN:

- **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 Private VLAN 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. There can be multiple distinct community VLANs within one Private VLAN domain.

There are mainly two types of ports in a Private VLAN: Promiscuous port (P-Port) and Host port.

- **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 in 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.

Private VLAN Example

1. Enabling a Private VLAN:

```
config switch vlan
edit 1000
    set private-vlan enable
    set isolated-vlan 101
    set community-vlans 200-210
end
end
```

2. Configuring the Private VLAN 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
```

Configuring SNMP Access

1. Ensure that the management vlan has SNMP added to the access-profiles:

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

2. Ensure that a SNMP community is created (with host configured):

```
config system snmp community
    edit <id>
        config hosts
            edit <id>
                end
            set name <name>
        end
    end
```

Layer 3 Interfaces

This chapter provides information about configuring Layer 3 interfaces. Fortinet data center switches support Switched Virtual Interfaces (SVI) and Routed Ports. These interface types are described in detail below.

Switched Virtual Interfaces

Switched Virtual Interface (or SVI) is a logical interface that is associated with a VLAN. You can assign an IP address to the SVI interface to enable routing between VLANs. For example, we may use SVIs to route between two different VLANs connected to a switch (no need to connect through a L3 router).

The SVI attaches to the "internal" interface in the switch. An SVI supports routing and switching protocols.

Configuring a Switched Virtual Interface

Using the CLI:

Set the Allowed VLAN list on the internal interface. Include all of the VLANs for ports that route through this SVI.

```
config switch interface
  edit internal
    set allowed-vlans <vlan list>
  end
```

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 interface internal
    set allowaccess ping ssh telnet
```

Configure a static route:

```
config router static
  edit 1
    set dst <IP subnet and mask>
    set device <system interface name>
```

Example SVI Configuration

The following is an example CLI configurations for SVI static routing.

In this configuration, Server-1 is connected to switch Port1 and Server-2 is connected to switch Port2. Their IP and MAC address are show in the diagram. Port1 is a member of VLAN 4000 and Port2 is a member of VLAN 2.

For Server-1, Port1 is the gateway and for Server-2, port2 is the gateway.

(Note: For simplicity, assume that both port1 and port are on same switch)

1. Configure Native VLANs for Port1 & Port2. Also configure “internal” interface to allow the native VLANs for Port1 and Port2.:

```
config switch interface
  edit port1
    set native-vlan 4000
  edit port2
    set native-vlan 2
  edit internal
    set allowed-vlans 2, 4000
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 interface internal
    set allowaccess ping ssh telnet
  next
  edit vlan2
    set ip 192.168.10.1/24
    set vlanid 2
    set interface internal
    set allowaccess ping ssh telnet
end
```

3. Configure static routes, so that the switch will know how to route between the two VLANs:

```
config router static
  edit 1
    set dst 192.168.10.0/24
    set device vlan2
  next
  edit 2
    set dst 192.168.11.0/24
    set device vlan4000
end
```

Viewing SVI Configuration

Display the status of SVI configuration using following command:

```
show system interface [ <system interface name> ]
```

Routed Interfaces

A routed port is a physical port on a switch that acts like a port on a router. It supports all routing protocols and terminates Layer 2 completely. It does not support VLAN sub-interfaces and it is not associated with a VLAN. A routed port typically connects to either a server or a router (a Layer 3 device).

The routed port is associated with a subnet.

The main reason to use a routed interface is to simplify the network topology.

Configuring a Routed Interface

Using the CLI:

Set the Allowed VLAN list on the internal interface. Include the VLANs of the routed ports.

```
config switch interface
  edit internal
    set allowed-vlans <vlan list>
  end
```

Create a Layer 3 virtual interface corresponding to the physical port:

```
config system interface
  edit <rvi name>
    set switch-members <port> <port> ...
  next
  edit <virtual device name>
    set vlanid <vlan>
    set ip <ip subnet> <mask>
    set interface <rvi name>
    set allowaccess ping telnet
```

Configure static routes, so that the switch will know how to route between VLANs:

```
config router static
  edit 2
    set device <virtual device name>
    set dst <ip subnet>
```

Example Routed Port Configuration

The following is an example CLI configuration for Routed Port static routing.

In this configuration, we configure Port2 and Port6 as a Routed Port. We created interface I-RED and I-GREEN as RVI interface. Remainder of the ports in the switch are normal Layer 2 ports.

1. Configure Native VLANs for Port2, Port6 and Port9. Also configure "internal" interface to allow native VLANs for Port2, Port6 and Port9.:

```
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. Create L3 virtual interfaces corresponding to the physical ports:

```
config system interface
  edit "i-red"
    set switch-members "port2"
  next
```

```

edit "i-green"
  set switch-members "port6"
next
edit "rVlan10"
  set vlanid 10
  set ip 1.1.3.1 255.255.255.0
  set interface "i-red"
  set allowaccess ping telnet
next
edit "gVlan20"
  set vlanid 20
  set ip 172.168.13.1 255.255.255.0
  set allowaccess ping telnet
  set interface "i-green"
next
edit "b-vlan30"
  set vlanid 30
  set ip 192.168.13.1 255.255.255.0
  set allowaccess ping telnet
  set interface internal
end

```

3. Configure static routes, so that the switch will know how to route between the two VLANs:

```

config router static
edit 1
  set device "mgmt"
  set gateway 10.105.0.1
next
edit 2
  set device "rVlan10"
  set dst 1.1.3.0/24
next
edit 3
  set device "gVlan20"
  set dst 172.168.13.0/24
next
edit 4
  set device "b-vlan30"
  set dst 192.168.13.0/24
end

```

Viewing Routed Port Configuration

Display the status of RVI configuration using following commands

```
show system interface [ <system interface name> ]
```

Layer 3 Routing in Hardware

In Release 3.3.0 and later releases, some FortiSwitch models support hardware-based Layer 3 forwarding.

For FortiSwitch models that support ECMP (see the feature matrix in the Introduction chapter), 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 will be forwarded by the hardware.

Equal Cost Multi-Path (ECMP) Routing

Equal Cost Multi-Path (ECMP) is a forwarding mechanism that enablee 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, or Input Port.

Configuring ECMP

The switch will automatically use ECMP to choose between equal-cost routes.

As input to the hash, you can configure the switch to use one or more of the following fields in the packet to be routed: Source IP, Destination IP, or Input Port.

This configuration value is system-wide. Source IP is the default value.

Notes and Restrictions

Maximum of 8 alternative paths (ie. ECMP paths).

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 be equal to 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, we configure Port2 and Port6 as routed ports. We create interfaces I-RED and I-GREEN as RVI interface. The remaining ports in the switch are normal Layer 2 ports.

1. Configure Native VLANs for Port2, Port6 and Port9. Also configure "internal" interface to allow native VLANs for Port2, Port6 and Port9.:

```
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 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. We are configuring multiple next hop gateway for the same network:

```
config router static
edit 1
set device "mgmt"
set gateway 10.105.0.1
next
edit 2
set device "i-red"
set dst 8.8.8.0/24
set gateway 172.16.11.2
next
edit 3
set device "i-green"
set dst 8.8.8.0/24
set gateway 172.168.13.2
next
```

Viewing ECMP Configuration

Display the status of ECMP configuration using following commands

```
show system interface [ <system interface name> ]
```

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is 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, MPLS LSP/PW).

BFD defines Demand mode and Asynchronous mode operation. The FortiSwitch 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 1-100,000 ms. Default value is 1000.
 - 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. Value range is 1-100,000 ms. Default value is 1000.
 - Detect multi. This is the detection time multiplier. The negotiated transmit interval multiplied by this value is the Detection Time for the receiving system.
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..50]
  next
config router static
  set bfd enable
```

Viewing BFD Configuration

Display the status of BFD sessions using following commands

```
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 detail:

```
get router info bfd neighbor detail
```

IP-MAC Binding

Use IP-MAC binding to prevent ARP spoofing.

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. Configure switch 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 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 default is for the trunk to follow the global value. You can also explicitly enable or disable IP-MAC binding for a trunk, as shown above.

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 allowed in the mapping table.

Rules are disabled by default. You need to explicitly enable each rule.

Mapping table holds up to 1024 rules.

Viewing IP-MAC Binding Configuration

Display the status of IP-MAC binding using following command

```
show switch ip-mac-binding <entry number>
```

802.1x Authentication

This chapter contains information about how to use IEEE 802.1x authentication on Fortinet switches.

About 802.1x

FortiSwitch supports IEEE 802.1x authentication to control network access. FortiSwitch implements port-based and MAC-based access.

A supplicant connected to a port on the switch must be authenticated by a Radius/diameter server in order to gain access to the network. The supplicant and the authentication server communicate via the switch using EAP protocol.

With port-based authentication, any user on the authenticated port will have access to the network.

With MAC-based authentication, the switch saves the MAC address of the supplicant's device. The switch limits network access to devices that have successfully been authenticated.

Authenticating a Remote Admin with RADIUS

Using the CLI:

1. Creating 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. Creating a user:

```
config user radius
  edit "RADIUS1"
    set secret
  next
end
```

3. Creating a user group:

```
config user group
  edit "RADIUS_Admins"
    set member "RADIUS1"
  next
end
```

Authenticating with a RADIUS server

Using the CLI:

1. Creating a RADIUS user group:

```
config user radius
  edit <name>
    set server <address>
  end
end
```

2. Creating 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. Configuring the switch interface for port-based 802.1x

```
config switch interface
  edit <interface>
    set security-mode 802.1X
    set security-groups <name>
  end
end
```

4. Configuring the switch interface for MAC-based 802.1x

```
config switch interface
  edit <interface>
    set security-mode 802.1X-mac-base
    set security-groups <name>
  end
end
```

5. Configuring an STP instance

```
config switch stp instance
  edit <name>
    set priority <integer>
  end
end
```

Using the web-based manager:

NOTE: Define the Radius server and remote user group using the CLI (steps 1 and 2 above).

1. Go to **Switch > Interface > Interface** and select the port to update.
2. Set **Security Mode** to either **802.1x** or **802.1x-mac-based**
3. Select **OK**.

Example Configuration

The following is an example configuration for a RADIUS user group, with the CLI syntax shown to create it.

1. Creating a RADIUS user group

```
config user radius
  edit R1
    set server "192.160.10.98"
  next
end
```

2. Creating a user group

```
config user group
  edit 802group
    set member user1 R1
    config match
      edit 1
        set group-name 802group
        set server-name R1
      end
    end
  end
end
```

TACACS

This chapter contains information on using TACACS authentication with your FortiSwitch unit.

Administrative Accounts

Administrative, or admin, accounts allow access to various aspects of the FortiSwitch configuration. The level of access is determined by the access profile used in the admin account.

Configuring an Access Profile for Admin Accounts

Using the web-based manager:

1. Go to **System > Admin > Admin Profile** and select **Create New**.
2. Give the profile an appropriate name.
3. Set **Access Control** as desired, choosing between **None**, **Read Only**, or **Read-Write**.
4. Select **OK**.

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
```

Configuring a TACACS Admin Account

Using the web-based manager:

1. Go to **System > Admin > Administrators** and select **Create New**.
2. Give the administrator account an appropriate name.
3. Set **Type** as **Remote**.
4. Set **User Group** to a group for remote users.
5. Enable **Wildcard**.
6. Set **Admin Profile** to use the new profile.
7. Select **OK**.

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 can be used to 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

This chapter covers tips and best practices for troubleshooting and support.

TFTP Network Port

When you power on the FortiSwitch, 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.

Set 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>
```

To list all of the flash partitions:

```
diagnose sys flash list
```

FORTINET

High Performance Network Security



Copyright© (Undefined variable: FortinetVariables.Year) Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.