



FortiSwitch-500

Version 4.0 MR1

Configuration Guide

Version 4.0 MR1

Revision 1

23 November 2009

© Copyright 2009 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS

CAUTION: Risk of explosion if battery is replaced by incorrect type. Dispose of used batteries according to Instructions.

Table of Contents

1 INTRODUCTION	6
1.1 Scope.....	6
1.2 Audience	6
1.3 Registering your Fortinet product.....	6
1.4 Customer Service and Technical Support.....	6
1.5 Training	7
1.6 Fortinet Documentation.....	7
1.7 Accessing the CLI	7
2 MANAGEMENT IP ADDRESS CONFIGURATION	9
2.1 Management and IP Addressing Options.....	9
2.1.1 In-band vs. Out-of-Band Management.....	9
2.1.2 DHCP vs. Static IP Addressing	9
2.2 IP Address Configuration.....	9
2.2.1 Configuring an IP Address via DHCP.....	9
2.2.2 Manually Configuring a Static IP Address.....	9
3 VLAN CONFIGURATION.....	11
3.1 VLAN Overview	11
3.1.1 Static vs. Dynamic VLANs.....	11
3.1.2 Viewing VLAN Information.....	11
3.2 Static VLANs.....	11
3.2.1 Manually Creating a Static VLAN	11
3.2.2 Removing a Static VLAN	12
3.2.3 Adding a Port or LAG to a VLAN	12
3.2.4 Adding All Ports to a VLAN.....	12
3.2.5 Dropping Untagged Ingress Frames	13
3.2.6 Changing the VLAN ID Assigned to Untagged Ingress Frames	13
3.3 Dynamic VLANs	13
3.3.1 Enabling GVRP on All Ports.....	14
3.3.2 Enabling GVRP on a Single Port.....	14
3.3.3 Enabling GVRP on a LAG	14
4 LAG CONFIGURATION.....	15

4.1 LAG Overview	15
4.1.1 LAGs Supersede Ports.....	15
4.1.2 LACP	15
4.2 LAG Configuration	15
4.2.1 Creating a LAG	15
4.2.2 Enabling GVRP on a LAG	15
4.2.3 Displaying LAG Information.....	16
5 SPANNING TREE CONFIGURATION	17
5.1 Spanning Tree Overview	17
5.2 Configuring Spanning Tree	17
5.2.1 Configuring STP (802.1D)	17
5.2.2 Configuring RSTP (802.1w).....	17
5.2.3 Configuring MSTP (802.1s).....	18
6 PORT MIRROR (MONITOR) CONFIGURATION	19
6.1 Port Mirroring Overview	19
6.2 Configuring Port Mirroring	19
6.2.1 Creating a Port Mirror	19
6.2.2 Viewing Mirror Settings.....	19
7 SNMP CONFIGURATION	20
7.1 SNMP Community Creation	20
7.1.1 Creating an SNMP Community	20
7.1.2 Controlling Access to an SNMP Community	20
7.1.3 Disabling and Enabling an Existing SNMP Community	21
7.2 SNMP Trap Configuration	21
7.2.1 Available SNMP Traps	21
7.2.2 Configuring SNMP Traps.....	21
7.3 Security Issues	22
8 LOGGING CONFIGURATION	23
8.1 Logging Overview	23
8.2 Configuring Logging	23
8.2.1 Severity Levels	23
8.2.2 Configuring Buffered Logging.....	23
8.2.3 Configuring Syslog Logging.....	24
8.2.4 Configuring CLI Command Logging	24

8.2.5 Configuring Console Logging	24
9 USERS AND AUTHENTICATION	26
9.1 Users and Authentication Overview	26
9.2 User Configuration.....	26
9.2.1 Adding Users to the Switch	26
9.2.2 Removing Users from the Switch	26
9.2.3 Viewing User Information	26
9.3 Authentication Configuration	26
9.3.1 Configuring RADIUS Server Authentication	27
9.3.2 Viewing Authentication Information	27
10 IPFIX CONFIGURATION	29
10.1 IPFIX Overview	29
10.2 IPFIX Configuration.....	29
10.2.1 Configuring IPFIX	29
10.2.2 Viewing IPFIX Information	29
11 SETTING UP PARTITIONS	30
11.1 Partitioning Overview	30
11.2 Partition Configuration.....	30
11.2.1 Creating Partitions for VLAN Segregation.....	30
11.2.2 Creating Partitions for Priority Segregation	31
11.2.3 Viewing Partition Information.....	31
12 FILE MANAGEMENT	32
12.1 File Management Overview	32
12.2 Basic File Operations	32
12.2.1 Listing the Contents of the Internal Flash Drive	32
12.2.2 Saving the Running Configuration.....	32
12.2.3 Resetting the Configuration to Factory Defaults	32
12.2.4 Deleting Files	32
12.2.5 Transferring Files.....	32
12.3 System Upgrades.....	33
12.3.1 Upgrading the System	33

1 Introduction

1.1 Scope

This document describes the tasks commonly performed in configuring the FortiSwitch-500 Ethernet Fabric Switch. Additional information regarding the FortiSwitch-500 is found in the following documents:

- **FortiSwitch-500 Install Guide** Installation procedures for the FortiSwitch-500 unit
- **FortiSwitch-500 CLI Reference** Full description of the FortiSwitch-500 CLI commands

1.2 Audience

This guide is intended for use by data center administrators, system administrators, customer support personnel and others responsible for configuring the FortiSwitch-500 Switch via the command line interface. It assumes a basic familiarity with the following:

- Network administration
- Establishing and using a telnet session
- Using a command line interface

1.3 Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article [Registration Frequently Asked Questions](#).

1.4 Customer Service and Technical Support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article [What does Fortinet Technical Support require in order to best assist the customer?](#)

1.5 Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email them at training@fortinet.com.

1.6 Fortinet Documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

1.6.1.1 Fortinet Tools & Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

1.6.1.2 Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

1.6.1.3 Comments on FortiMail technical documentation

Please send information about any errors or omissions in this document to techdoc@fortinet.com.

1.7 Accessing the CLI

The CLI is accessed via:

- Serial interface connected directly from a PC to the serial console port of the switch
- Telnet session or secure shell (SSH) session. Telnet or SSH session can be initiated in-band through the network or out-of-band via the management network port; either telnet or SSH access requires that an IP address be configured on the switch (see Management IP Address Configuration on page 9).

Note: The maximum number of concurrent telnet and SSH connections to the switch is 15.

The following are the default settings of these interfaces:

- **Serial:** initialized baud-rate 115200, 8 bit, no parity, and no flow control. By default the serial port is turned on.
- **Telnet:** initialized to port 23. By default the telnet service is turned on.

-
- **SSH:** initialized to port 22. By default the SSH service is turned off.

2 Management IP Address Configuration

In order to configure or otherwise manage the FortiSwitch-500 without the use of a console directly attached to the serial console port, an IP address must first be configured on the switch to allow access via telnet or SSH session.

2.1 Management and IP Addressing Options

2.1.1 In-band vs. Out-of-Band Management

The FortiSwitch-500 may be managed in-band or out-of-band, with out-of-band management typically being performed via the management port on the front of the switch. Fortinet recommends use of out-of-band management to allow uninterrupted access to the switch in the event of a broadcast storm.

2.1.2 DHCP vs. Static IP Addressing

In order to ensure out-of-the-crate functionality, the FortiSwitch-500 is configured to seek an IP address via DHCP by default, but a static IP address can also easily be manually configured on the switch. If the network administrator wishes to always access the switch by a consistent IP address, Fortinet recommends manually configuring a static management IP address.

2.2 IP Address Configuration

2.2.1 Configuring an IP Address via DHCP

2.2.1.1 Setting the IP Address

By default, the FortiSwitch-500 will attempt to acquire an IP address automatically via DHCP once the switch is running and a network cable is plugged into the management network port. If the management network port is connected to a network which includes a functioning DHCP server, an IP address for the management network port should be automatically configured on the switch.

2.2.1.2 Finding the Assigned IP Address

If the DHCP-assigned management IP address for the switch cannot be easily deduced from the network, it can be found through the CLI:

1. Log into the switch (see 2.2.2.1 below).
2. Type **show mgmt-ip service-port** to display configuration information for the management service port, including the management IP address.

2.2.2 Manually Configuring a Static IP Address

The process below assumes that the operator is configuring the switch for out-of-band management. In-band management is disabled on the switch by default; information on

configuring in-band management can be found in the *CLI Reference Guide* in the section describing the **mgmt-ip inband** command.

2.2.2.1 Logging in to the Switch

The switch is factory configured with a single administrator-level login account. To log in to the switch for the first time with administrative privileges:

1. Ensure that the switch has been turned on and allowed to boot up.
2. Connect a console to the serial console port (see page 6). The settings for the serial connection are an initialized baud-rate of 115200, 8 bit, no parity, and no flow control.
3. Type **admin** for the user name, and enter for the password (the default account has no associated password).

2.2.2.2 Setting the IP Address, Netmask and Gateway

Once logged in to the CLI, use the following steps to enter static IP address details for the management network port:

1. Type **enable** to enter Enable Mode.
2. Type **config** to enter Config Mode.
3. Type **mgmt-ip service-port ip <ip_address><netmask><gateway>** where *<ip_address>* is the static IP address you wish to configure on the management network port for out-of-band management of the switch.

3 VLAN Configuration

3.1 VLAN Overview

VLANs on the FortiSwitch-500 are of two distinct types, referred to as Service VLANs (SVLANs) and VLANs. SVLANs are the transparent VLANs used within the fabric for optimized traffic management. VLANs are user-configured VLANs which may extend outside the fabric. This section explains the configuration of VLANs (user-configured VLANs).

3.1.1 Static vs. Dynamic VLANs

By default, VLAN 1 is created on the FortiSwitch-500 as a static VLAN, and all interfaces on the FortiSwitch-500 participate in VLAN 1. For an interface to participate in any other VLAN, that VLAN must be created and the interface must be configured for participation in that VLAN. This can be done statically by manual creation of a static VLAN (which will persist over a reboot) and manual configuration of individual interfaces to participate in the VLAN, or dynamically via GARP VLAN Registration Protocol (GVRP).

A static VLAN is configurable and will persist over a reboot. VLAN 1 is a static VLAN, created automatically, and all interfaces on the switch participate in VLAN 1 by default; any other static VLAN must be either explicitly created or converted from a dynamic VLAN created by GVRP (see Dynamic VLANs on page 13, below). Only static VLANs may be edited or manually configured. If a VLAN is dynamically created by GVRP, participation of interfaces in the VLAN, tagging of egress traffic and other parameters cannot be configured unless the VLAN is made static. Also note that a static VLAN cannot be created with the same ID as a dynamic VLAN currently on the switch. If you need to make a dynamic VLAN static (for instance to configure it), use the **makestatic** option of the **vlan-id** command.

3.1.2 Viewing VLAN Information

To view all VLANs on the switch, use the **show vlan brief** command in Enable Mode. To see detailed information about a specific VLAN, use the **show vlan <1-4094>** command (also in Enable Mode), where **<1-4094>** is the ID of the VLAN you wish to view.

3.2 Static VLANs

3.2.1 Manually Creating a Static VLAN

1. From Enable Mode, type **config** and then **vlan** to enter Config-VLAN Mode.
2. Type **vlan-id<1-4094>** (where **<1-4094>** is a valid VLAN ID) to create a static VLAN of the specified ID. To create multiple VLANs, issue the command repeatedly with different IDs.

Note: if a dynamic VLAN already exists with the specified VLAN ID, this command will not work. To configure an existing dynamic VLAN, you must first use the **vlan-id makestatic** command in Config-VLAN Mode to convert the dynamic VLAN into a static VLAN.

Optional:

-
3. Type **vlan-id name** *<new_name>* (where *<new_name>* is the name chosen for the VLAN) to attach an arbitrary name to the VLAN. This can help identify the intent or purpose of the VLAN when it is listed in show commands. Note that before the VLAN can be named, it must be created first as a separate command.

3.2.2 Removing a Static VLAN

To remove a static VLAN from the VLAN database, use the “no” form of the **vlan-id** command: **no vlan-ID** *<1-4094>* in Enable Mode (where *<1-4094>* is the ID of the VLAN being removed).

3.2.3 Adding a Port or LAG to a VLAN

An interface (port or LAG) can be configured to participate in any static VLAN configured on the switch. However, interfaces cannot be assigned manually to a dynamic VLAN. In order to manually assign interfaces to a VLAN, the VLAN must either be the default VLAN (VLAN 1), be created statically, or be made static using the **vlan make-static** command in Config-VLAN Mode.

3.2.3.1 Adding a Port to a VLAN

1. From Enable Mode, type **config** and then **port** *<slot/port>* (where *<slot/port>* is the port to be added to the VLAN) to enter Config-Port Mode. (Note that on the FortiSwitch-500, the *slot* value is always “1”.)
2. Type **vlan participation include** *<1-4094>* (where *<1-4094>* is the VLAN ID of the static VLAN to which you wish to add this port) to add the port to the VLAN.
3. If you want egress packet tagging enabled for this VLAN on this port, type **vlan tagging** *<1-4094>* (where *<1-4094>* is the VLAN ID). Tagging is disabled by default.

3.2.3.2 Adding a LAG to a VLAN

1. From Enable Mode, type **config** and then **lag** *<1-12>* (where *<1-12>* is the LAG ID of the LAG to be added to the VLAN) to enter Config-LAG Mode.
2. Type **vlan participation include** *<1-4094>* (where *<1-4094>* is the VLAN ID of the static VLAN to which you wish to add this LAG) to add the LAG to the VLAN.
3. If you want egress packet tagging enabled for this VLAN on this LAG, type **vlan tagging** *<1-4094>* (where *<1-4094>* is the VLAN ID). Tagging is disabled by default.

3.2.4 Adding All Ports to a VLAN

While adding single interfaces to a VLAN must be done one at a time from the configuration mode for the interface, *all* switch ports can be configured to participate in a VLAN from Config-VLAN Mode in a single process. As above, note that interfaces can only be added manually to a static VLAN; the VLAN must be created statically, or be made static using the **vlan make-static** command in Config-VLAN mode.

To add all ports to a VLAN:

1. From Enable Mode, type **config** and then **vlan** to enter Config-VLAN Mode.
2. Type **participation all include** *<1-4094>* (where *<1-4094>* is the VLAN ID of the static VLAN to which you wish to add all switch ports) to add all ports on the switch to the VLAN.

All ports can likewise be removed from a VLAN by typing **participation all exclude** *<1-4094>* in Config-VLAN Mode.

3.2.5 Dropping Untagged Ingress Frames

By default, untagged frames received on any interface of the FortiSwitch-500 are accepted and given the native VLAN ID (1, by default) of the interface on which they entered the switch. All interfaces can, however, be configured to drop untagged frames.

Note: dropping untagged frames can cause problems with legacy devices that send and receive untagged frames as keepalives.

3.2.5.1 Dropping Untagged Frames (Port)

1. From Enable Mode, type **config** and then **port <slot/port>** (where *<slot/port>* is the slot and port which you wish to configure) to enter Config-Port Mode. Note that on the FortiSwitch-500, the *slot* value is always “1”.
2. Type **vlan acceptframe vlanonly**. (To accept untagged frames on the port again, type **vlan acceptframe all**.)

3.2.5.2 Dropping Untagged Frames (LAG)

3. From Enable Mode, type **config** and then **lag <1-12>** (where *<1-12>* is the LAG ID of the LAG which you wish to configure) to enter Config-LAG Mode.
4. Type **vlan acceptframe vlanonly**. (To accept untagged frames on the LAG again, type **vlan acceptframe all**.)

3.2.6 Changing the VLAN ID Assigned to Untagged Ingress Frames

By default, all interfaces on the FortiSwitch-500 accept untagged ingress frames and assign them a VLAN ID of 1. To assign a different VLAN ID to untagged frames received on a specific interface, you must ensure that the interface is configured to accept untagged frames and change the native VLAN ID of the interface.

3.2.6.1 Changing the Native VLAN ID of a Port

1. From Enable Mode, type **config** and then **port <slot/port>** (where *<slot/port>* is the slot and port which you wish to configure) to enter Config-Port Mode. Note that on the FortiSwitch-500, the *slot* value is always “1”.
2. Type **vlan acceptframe all** to ensure that the port is accepting untagged frames.
3. Type **vlan pvid <1-4094>**, where *<1-4094>* is the native VLAN ID which you would like to have assigned to untagged frames received on this port.

3.2.6.2 Changing the Native VLAN ID of a LAG

1. From Enable Mode, type **config** and then **LAG <1-12>** (where *<1-12>* is the ID of the LAG which you wish to configure) to enter Config-LAG Mode.
2. Type **vlan acceptframe all** to ensure that the LAG is accepting untagged frames.
3. Type **vlan pvid <1-4094>**, where *<1-4094>* is the native VLAN ID which you would like to have assigned to untagged frames received on this LAG.

3.3 Dynamic VLANs

For devices to communicate via a VLAN, each port between those devices must be configured to participate in that VLAN. The GARP VLAN Registration Protocol (GVRP) allows for dynamic

creation and configuration of VLANs so that the operator does not need to manually configure the pathway.

3.3.1 Enabling GVRP on All Ports

Note: For GVRP to function on a given port, it must be enabled on that port *and* on the switch as a whole. GVRP can be enabled on all ports simultaneously, or it can be enabled on a single port. Below are the steps to enable GVRP on all ports.

1. From Enable Mode, type **config** to enter Config Mode, then type **gvrp admin-mode** to enable GVRP globally on the switch.
2. Type **gvrp port-mode** to enable GVRP on every switch port.

3.3.2 Enabling GVRP on a Single Port

1. From Enable Mode, type **config** to enter Config Mode, then type **gvrp admin-mode** to enable GVRP globally on the switch.
2. From Enable Mode, type **config** and then **port <slot/port>** (where *<slot/port>* is the port which you wish to configure) to enter Config-Port Mode. Note that on the FortiSwitch-500 the *slot* value is always "1".
3. Type **vlan acceptframe all** to ensure that the port is accepting untagged frames.
4. Type **gvrp port-mode** to enable GVRP on the port.

To disable GVRP on a single port, follow the above steps but type **no gvrp port-mode** in the last step.

3.3.3 Enabling GVRP on a LAG

1. Create the LAG.
 - a. From Enable Mode, type **config** to enter Config Mode.
 - b. Type **lag <1-12>** (where *<1-12>* is the ID of the LAG you wish to create) to create the LAG and enter Config-LAG mode.
 - c. Type **add-port <slot/port>** (where *<slot/port>* is the port you wish to add to the LAG) to add a member port. Note that on the FortiSwitch-500 the *slot* value is always "1".
 - d. Repeat step c for each port to be added to the LAG.
2. Enable GVRP on the LAG. Still in Config-LAG Mode:
 - a. Type **vlan acceptframe all** to ensure that the LAG is accepting untagged frames.
 - b. Type **gvrp port-mode** to enable GVRP on the LAG.
3. Enable GVRP globally. Starting in Config-LAG Mode:
 - a. Type **exit** to exit to Config Mode.
 - b. Type **gvrp admin-mode** to enable GVRP globally on the switch.

4 LAG Configuration

4.1 LAG Overview

The FortiSwitch-500 uses the IEEE 802.1q LAG standard, allowing interoperability with all other switches, routers, servers and other devices that are 802.1q compliant.

LAGs can support up to 6 ports and are identified by a LAG ID number between 1 and 12.

4.1.1 LAGs Supersede Ports

LAG configuration commands supersede any configuration of the individual ports that make up the LAG; any port-level configuration persists on the individual ports, however, and takes control if those interfaces are removed from the LAG.

4.1.2 LACP

Link Aggregation Control Protocol (LACP) is always in operation on the FortiSwitch-500. If the FortiSwitch-500 is connected via a LAG to a device on which LACP is not enabled, the FortiSwitch-500 keeps all links up at all times. When connecting a device that has optional LACP to the FortiSwitch-500, Fortinet recommends that LACP be enabled on that device.

4.2 LAG Configuration

4.2.1 Creating a LAG

Note: when ports are assembled into a LAG, GVRP must be disabled on those ports; if ports with GVRP enabled are assembled into a LAG, that LAG will not pass traffic. For information on disabling GVRP on member ports, see section 4.2.2 below.

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **LAG <1-12>** (where <1-12> is a valid LAG ID) to create a LAG of the specified ID and enter Config-LAG Mode. (Note that the FortiSwitch-500 CLI uses a LAG ID number between 1 and 12 rather than the lowest port in the LAG as a reference for the LAG itself.)
3. Type **add-port <slot/port>** (where <slot/port> is a port which will belong to the LAG) to add a port to the LAG. This command must be repeated for each port to be added to the LAG. To remove a port from the LAG, type **delete-port <slot/port>** (where <slot/port> is the port which you are removing from the LAG). Note that on the FortiSwitch-500 the *slot* value is always "1".

4.2.2 Enabling GVRP on a LAG

When ports are assembled into a LAG, GVRP must be disabled on those ports; if ports with GVRP enabled are assembled into a LAG, that LAG will not pass traffic. To enable GVRP on a LAG, the individual member ports must have GVRP disabled before they are included in the LAG; then GVRP can be enabled on the LAG as a whole.

To enable GVRP on a LAG:

1. Disable GVRP on the member ports. The easiest way to do this globally: From Enable Mode, type **config** to enter Config Mode, then type **no gvrp port-mode** to disable GVRP on all ports of the switch. If it is necessary to disable GVRP on a port-by-port basis instead, though, do the following for each port:
 - c. From Config Mode, type **port <slot/port>** (where <slot/port> is the port on which you wish to disable GVRP) to enter Config-Port Mode. Note that on the FortiSwitch-500 the *slot* value is always "1".
 - d. Type **no gvrp port-mode** to disable GVRP on the port.
 - e. Type **exit** to return to Config Mode and repeat steps a and b for each additional port.
2. Create the LAG. Once GVRP is disabled on each member port, assemble the ports into a LAG. (Note that the FortiSwitch-500 CLI uses a LAG ID number between 1 and 12 rather than the lowest port in the LAG as a reference for the LAG itself.)
 - f. From Enable Mode, type **config** to enter Config Mode.
 - g. Type **lag <1-12>** (where <1-12> is the ID of the LAG you wish to create) to create the LAG and enter Config-LAG mode.
 - h. Type **add-port <slot/port>** (where <slot/port> is the port you wish to add to the LAG) to add a member port.
 - i. Repeat step c for each port to be added to the LAG.
3. Enable GVRP on the LAG. Still in Config-LAG Mode:
 - j. Type **vlan acceptframe all** to ensure that the LAG is accepting untagged frames.
 - k. Type **gvrp port-mode** to enable GVRP on the LAG.
4. Enable GVRP globally. Starting in Config-LAG Mode:
 - l. Type **exit** to exit to Config Mode.
 - m. Type **gvrp admin-mode** to enable GVRP globally on the switch.

Note: the order is essential in this process: if GVRP is already enabled on the member ports when they are included in a LAG, the LAG will not pass traffic.

4.2.3 Displaying LAG Information

show lag <1-12> (where <1-12> is the ID of the LAG) shows detailed information about the specified LAG, including a list of member ports. (Use **show lag all** to display the same information for all LAGs configured on the switch.)

show lag <1-12> lacp (where <1-12> is the ID of the LAG) shows Link Aggregation Control Protocol (LACP) information for the specified LAG.

show lag <1-12> vlan (where <1-12> is the ID of the LAG) shows VLAN configuration information for the specified LAG.

show lag brief displays LAG static capability and summary information for the switch as a whole.

5 Spanning Tree Configuration

5.1 Spanning Tree Overview

The FortiSwitch-500 supports STP (IEEE 802.1D), RSTP (IEEE 802.1w) and MSTP (IEEE 802.1s). By default, MSTP (802.1s) is enabled globally on the switch and spanning tree is enabled on all ports.

5.2 Configuring Spanning Tree

Note: three spanning tree protocols are supported by the FortiSwitch-500; the switch is configured differently depending on which spanning tree protocol is being used.

5.2.1 Configuring STP (802.1D)

1. Type **enable** to enter Enable Mode.
2. Type **config** to enter Config Mode.
3. Type **spanning-tree force-version 802.1d** to enable STP globally on the switch (if it has been disabled) and set the version to 802.1d.
4. Spanning tree is enabled by default on all ports; if it has been disabled on any participating port, enable it by typing **port <slot/port>** (where <slot/port> is the port on which spanning tree has been disabled), then type **spanning-tree port-mode** to enable spanning tree on the port.

To enable spanning tree on a range of ports, type **port range <slot/port> <slot/port>** (where the two <slot/port> variables identify the first and last ports in the range to be configured), then type **spanning-tree port-mode** to enable STP on each port within that range.

Note that on the FortiSwitch-500 the *slot* value is always "1".

Optional steps (all performed from Config Mode):

5. Change the forward time (set to 15 seconds by default). Type **spanning-tree forward-time <4-30>**, where <4-30> is the bridge forward delay time in seconds. Value must be greater than or equal to $(\text{bridge max age} / 2) + 1$.
6. Change the hello time (set to 2 seconds by default). Type **spanning-tree hello-time <1-10>**, where <1-10> is the hello time in seconds. Value must be less than or equal to $(\text{bridge max age} / 2) - 1$.
7. Change the maximum bridge age (set to 20 seconds by default). Type **spanning-tree max-age <6-40>**, where <6-40> is the bridge max age in seconds. Value must be less than or equal to $2 * (\text{bridge forward delay time} - 1)$.

5.2.2 Configuring RSTP (802.1w)

RSTP configuration is identical to STP configuration (above) except for the version number: follow the steps for STP configuration, but type **spanning-tree force-version 802.1w** in step 3.

5.2.3 Configuring MSTP (802.1s)

1. Type **enable** to enter Enable Mode.
2. Type **config** to enter Config Mode.
3. Type **spanning-tree force-version 802.1s** to enable spanning tree globally on the switch (if it has been disabled) and set the version to 802.1s (MSTP).
4. Spanning tree is enabled by default on all ports; if it has been disabled on any participating port, enable it by typing **port <slot/port>** (where <slot/port> is the port on which STP has been disabled), then type **spanning-tree port-mode** to enable STP on the port.

To enable spanning tree on a range of ports, type **port range <slot/port> <slot/port>** (where the two <slot/port> variables identify the first and last ports in the range to be configured), then type **spanning-tree port-mode** to enable STP on each port within that range.

Note that on the FortiSwitch-500 the *slot* value is always “1”.

5. Type **spanning-tree mst instance <1-4094>** (where <1-4094> is the identifier of the MST instance) to create an MST instance. (Only MST instance 0 is defined by default, and all configured VLANs are mapped to instance 0.)
6. Map VLANs to the MST instance. Type **mst <0-4094> vlan <1-4094>** (where <0-4094> is the MST instance identifier and <1-4094> is the VLAN ID) to add a VLAN to the MST instance. To add multiple VLANs, repeat the command for each VLAN to be added. Using MST instance 0 indicates that there is only a single spanning tree in operation.
7. Set the name and configuration to complete the definition of the MST region. Type **spanning-tree configuration name <name>** (where <name> is the name for the configuration the switch is using), then type **spanning-tree configuration revision <0-65535>** (where <0-65535> is the configuration identifier revision level).

Optional Steps:

8. The default bridge priority is set to 32768 by default. You may set the bridge priority for an MST instance to a different value by typing **spanning-tree mst <0-4094> priority <0-61440>** (where <0-4094> is the spanning tree instance and <0-65535> is the bridge priority).
9. The priority of all ports in relation to the MST instance is set at 128 by default. You may change the port priority value of a given port by typing **port <slot/port>** (where <slot/port> is the port whose priority is being set), then typing **spanning-tree mst <1-4094> port-priority <0-240>** (where <1-4094> is the MST instance and <0-240> is the priority for the port used by the specified MST instance).

6 Port Mirror (Monitor) Configuration

6.1 Port Mirroring Overview

Port mirroring forwards a copy of each incoming or outgoing packet (or both) from one port of a switch to another port where the packet can be studied. Mirroring does not affect the client on the original port.

Multiple port mirrors are supported on the FortiSwitch-500 up to the following maxima:

- **5 mirrors per destination** (i.e., one port can be configured to mirror up to five other ports on the same switch)
- **2 destinations per switch** (i.e., two different ports on a single FortiSwitch-500 can be configured to mirror other ports)

6.2 Configuring Port Mirroring

Port mirror configuration on the FortiSwitch-500 is done on the destination port (i.e., a port mirror is configured in Config-Port Mode on the port to which the duplicate packets will be sent).

6.2.1 Creating a Port Mirror

1. From Enable Mode, type **config** and then **port <slot/port>** (where <slot/port> is the destination port to which you want duplicate packets sent) to enter Config-Port Mode. (Note that on the FortiSwitch-500, the *slot* value is always "1".) Determine whether you want to mirror duplicates of packets received on the monitored port, packets transmitted by the monitored port or both.
 - a. To mirror only packets received, type **monitor <slot/port> rx**, where <slot/port> is the port which you wish to monitor.
 - b. To mirror only packets transmitted, type **monitor <slot/port> tx**, where <slot/port> is the port which you wish to monitor.
 - c. To mirror all packets, type **monitor <slot/port> both**, where <slot/port> is the port which you wish to monitor.

6.2.2 Viewing Mirror Settings

To view mirror settings, from Enable Mode type **show monitor**. This displays a list of all mirrors configured on the switch, their source and destination ports, and which packets are being mirrored (transmit, receive or both).

7 SNMP Configuration

7.1 SNMP Community Creation

There are no default SNMP communities enabled on the FortiSwitch-500. To use SNMP, the operator must create one or more SNMP communities on the switch.

7.1.1 Creating an SNMP Community

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **snmpd community <community_name>** (where <community_name> is the name you have chosen for the SNMP community). This both creates the community and assigns the name to it.

Optional Steps:

3. If you wish to set the access level of the custom community to read-write, type **snmpd community rw <community_name>**.
Note: The access level of a new SNMP community is set to read-only by default; this step is generally used only to set access to read-write. However, to explicitly set an SNMP community's access level to read-only, use the command **snmpd community ro <community_name>**.
4. To enter contact information for the switch, type **snmpd contact <contact_name>** (where <contact_name> is the SNMP contact information, up to 31 characters in length).
5. To enter location information for the switch, type **snmpd location <location>** (where <location> is a description of the physical location of the switch, up to 31 characters in length).
6. To enter a system name, type **snmpd sysname <system_name>** (where <system_name> is the system name, up to 31 characters in length).

7.1.2 Controlling Access to an SNMP Community

An SNMP community is created as a read-only community accessible from any IP address. Access can be limited by specifying an exclusive range of IP addresses which are allowed to query the SNMP community (one range per community), and greater control may be granted by making the community read-write.

7.1.2.1 Limiting Which IP Addresses Are Allowed to Query the Switch Via SNMP

1. Type **snmpd community ipaddr <ip_address> <community_name>** (where <ip_address> is the IP address of the SNMP client allowed to query the community, and <community_name> is the name of the SNMP community).
2. Input the subnet mask of the range of IP addresses allowed to access the SNMP community by typing **snmpd community ipmask <ip_mask> <community_name>** (where <ip_mask> is the client's subnet mask and <community_name> is the name of the SNMP community).

7.1.2.2 Allowing Read-Write Access to an SNMP Community

Type `snmpd community rw <community_name>`

7.1.3 Disabling and Enabling an Existing SNMP Community

To disable an existing SNMP community, type `no snmpd community mode <community_name>` where `<community_name>` is the name of the SNMP community you wish to disable. To enable the community again, type `snmpd community mode <community_name>`.

7.2 SNMP Trap Configuration

Five SNMP traps are configured by default on the FortiSwitch-500. Users can also configure up to five additional custom SNMP traps – either standard SNMP traps as defined in RFC 1157, or uptime traps for SNMP communities configured on the switch. To create an SNMP trap, the trap must be enabled and a receiver for the trap must be configured.

7.2.1 Available SNMP Traps

There are five SNMP traps configured and enabled by default on the FortiSwitch-500:

- **authentication** authentication trap
- **bcaststorm** broadcast storm trap
- **linkmode** equivalent to a combination of the standard linkDown and linkUp traps
- **multiusers** simultaneous login trap
- **stp-mode** STP trap

The FortiSwitch-500 also recognizes some of the standard SNMP traps as described in RFC 1157:

- **coldStart**
- **warmStart**
- **linkDown**
- **linkUp**
- **egpNeighborLoss**

Finally, the operator may also configure an uptime trap for any SNMP community configured on the switch, as detailed below.

7.2.2 Configuring SNMP Traps

Default Traps

The five default SNMP traps mentioned above are enabled by default. If one has been disabled, follow these steps to re-enable it:

1. From Enable Mode, type `config` to enter Config Mode.

-
2. Type **snmpd enable-traps** *<trap_name>* (where *<trap_name>* is the name of the FortiSwitch SNMP trap: authentication, bcaststorm, linkmode, multiusers or stp-mode) to enable the desired trap.

Custom Traps

In addition to the five default traps, up to five custom SNMP traps can be configured on the FortiSwitch-500.

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **snmp-trap** *<trap_name>* *<ip_address>* to create the custom trap. The value for *<trap_name>* should be one of the five standard RFC-defined SNMP traps listed above, or the name of an SNMP community configured on the switch. (Using the name of an SNMP community sets a trap which sends uptime information for that community.) The value for *<ip_address>* is the IP address of the SNMP server to which the traps are to be sent.
3. Type **snmp-trap mode** *<trap_name>* *<ip_address>* (where *<trap_name>* is the name of the trap created in step 2 and *<ip_address>* is the IP address of the SNMP server) to enable the custom trap.

Optional:

4. FortiSwitch-500 SNMP traps are set to SNMP version 2 by default; if you are using a trap receiver which requires SNMP version 1 traps, set the SNMP version of the custom trap to 1 by typing **snmp-trap snmp-version** *<trap_name>* *<ip_address>* **snmpv1** (where *<trap_name>* is the name of the custom trap and *<ip_address>* is the management IP address of the switch).

7.3 Security Issues

To increase system security, Fortinet recommends avoiding the use of “public” and “private” as community string names, and these community strings are not enabled by default. If you are using older configuration files that depend on these default communities, Fortinet recommends altering your configuration file to create new custom community strings and updating the configuration to use the new string names.

8 Logging Configuration

8.1 Logging Overview

Event messages generated by the FortiSwitch-500 can be logged directly to the console, to a remote syslog, or into an ephemeral buffer. All commands typed into the CLI can also be logged.

8.2 Configuring Logging

There are three primary methods of logging available on the FortiSwitch-500:

- Buffered logging is ephemeral and of limited size and is cleared on reboot.
- Syslog logging is logged to an external server.
- Console logging logs event messages directly to the console.

In addition to these three methods of logging, the FortiSwitch-500 can be configured to log all CLI commands typed.

All logging is configured using the **logging** command in Config Mode. From Enable Mode, start by typing **config** to enter Config Mode.

8.2.1 Severity Levels

For several of the logging options, you may specify a severity level filter for system event messages; lower levels output fewer events. The levels are as follows:

0: emergency, 1: alert, 2: critical, 3: error, 4: warning, 5: notice, 6: informational, 7: debug

For logging configuration, severity levels can be entered by name (“emergency,” “alert,” etc.) or by number.

8.2.2 Configuring Buffered Logging

Buffered logging logs system event messages into an ephemeral buffer which holds approximately 1000 lines. Newer messages displace older messages once the buffer is full, and the buffer is cleared on reboot. Buffered logging is enabled by default, and the severity level is fixed at level 6 (“informational”) and cannot be configured.

8.2.2.1 Enabling Buffered Logging

From Config Mode, type **logging buffered [wrap]** to enable buffered logging. The **wrap** option enables line-wrapping on log entries that exceed the size of the line buffer.

8.2.2.2 Disabling Buffered Logging

From Config Mode, type **no logging buffered**.

8.2.2.3 Clearing the Buffered Log

From Config Mode, type **clear logging buffered**

8.2.2.4 Viewing the Entries in the Buffered Log

From Enable Mode (not Config Mode), type **show logging buffered**

8.2.3 Configuring Syslog Logging

Syslog logging relays system event messages to a remote syslog server. By default, syslog logging is disabled, and the severity level is configured to 7 (debug).

8.2.3.1 Enabling Syslog Logging

From Config Mode, type **logging syslog** to enable syslog logging.

8.2.3.2 Disabling Syslog Logging

From Config Mode type **no logging syslog**

8.2.3.3 Specifying a Port For Syslog Monitoring

From Config Mode, type **logging syslog port <port_ID>** (where <port_ID> is the port to be monitored). If not specified, the default is 514.

8.2.3.4 Configuring a Host For Receiving Syslog Messages

From Config Mode, type **logging host <ip_address> [port_ID] [severity_level]**, where <ip_address> is the IP address of the host device for the configured syslog server that is to receive syslog messages relayed from the switch. The default port is 514.

The optional [severity_level] variable specifies the minimum severity level required for a system message to be sent to the syslog. (See 8.2.1 above for a description of the severity levels.)

8.2.4 Configuring CLI Command Logging

CLI command logging logs all commands executed via the command line interface. CLI command logging is enabled by default.

8.2.4.1 Enabling CLI Command Logging

From Config Mode, type **logging cli-command** to enable CLI command logging.

8.2.4.2 Disabling CLI Command Logging

From Config Mode, type **no logging cli-command**.

8.2.5 Configuring Console Logging

Console logging logs all system events to a serial console attached to the switch. This is used primarily in debugging scenarios when the operator needs to monitor all system events in real time. Console logging is disabled by default. The severity filter defaults to level 1 (“alert”) and is configurable.

Note: Console logging at “debug” level may send an overwhelming volume of messages to the console. Even at lower severity levels, sending logging output to the console can make it difficult to regain control of the switch if no other mode of access (e.g., telnet) is available.

8.2.5.1 Enabling Console Logging

From Config Mode, type **logging console [severity_level]** (where [severity_level] is the optional logging severity level – default is “alert”) to enable console logging.

8.2.5.2 Disabling Console Logging

From Config Mode, type **no logging console** to disable console logging.

9 Users and Authentication

9.1 Users and Authentication Overview

Up to five custom user accounts may be configured on the FortiSwitch-500, with authentication being administered either on the switch itself or via a remote authentication server.

9.2 User Configuration

The factory settings for the FortiSwitch-500 include a read/write user account named “admin” and a read-only account named “guest,” both of which are configured by default with no password. Four additional custom users may be added to the switch, and the “guest” account may be deleted and replaced with a fifth custom user. The default “admin” account cannot be removed or renamed, but can and should have a password assigned to it for security purposes.

9.2.1 Adding Users to the Switch

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **users name** *<user_name>* (where *<user_name>* is the name of the user being added) to create a new user account.
3. If you wish to protect access to the new account with a password, type **users password** *<user_name>* (where *<user_name>* is the name of the user created above). You will be prompted to enter old and new passwords; for a newly created user, there is no old password (press enter for a blank password).
4. The default access mode for the newly-created user account is read-only. To set the access mode to read/write, type **users access-mode** *<user_name>* **readwrite**.

9.2.2 Removing Users from the Switch

To remove a user account, from Config Mode type **no users name** *<user_name>* (where *<user_name>* is the name of the user you wish to remove from the switch).

9.2.3 Viewing User Information

To see a list of users configured on the switch, from Enable Mode type **show users**.

9.3 Authentication Configuration

Default user authentication is performed locally on the FortiSwitch-500, but the switch also supports external Remote Authentication Dial In User Service (RADIUS) server authentication.

9.3.1 Configuring RADIUS Server Authentication

When a new user is created on the FortiSwitch-500, they are added automatically to the default login list and will be authenticated locally on the switch without further configuration.

If you choose to use external RADIUS server authentication instead, follow these steps:

1. From Enable Mode, type **config** to enter Config Mode.
2. Create a custom authentication list. From Config Mode, type **authentication login** *<list_name>* **radius** (where *<list_name>* is the name you've chosen for the new authentication list). The **radius** option specifies that users on this list will be authenticated using an external RADIUS server.
3. Add users to be authenticated by the RADIUS server to the list. For each user to be added, type **users login** *<user_name>* *<list_name>* (where *<user_name>* is the name of the user to be added to the list and *<list_name>* is the name of the custom authentication list created in step 2 above).
4. Configure the IP address for the RADIUS authentication server. From Config Mode, type **radius server host auth** *<ip_address>* [*0-65535*] (where *<ip_address>* is the IP address of the authentication server). The optional value [*0-65535*] is the UDP port to be used in connecting to the RADIUS server; if no value is set here, the default is 1812.

For further RADIUS configuration (including accounting server configuration), please see the CLI Command Reference Guide.

9.3.2 Viewing Authentication Information

Authentication information may be viewed from Enable Mode using any of the following commands:

show users

	SNMPv3	SNMPv3	SNMPv3	
User Name	User Access Mode	Access Mode	Authentication	Encryption
admin	Read/Write	Read/Write	None	None
guest	Read Only	Read Only	None	None

show users authentication

Authentication Login Lists

User	System Login	802.1x
admin	defaultList	defaultList
guest	defaultList	defaultList
default	defaultList	defaultList

show authentication

Authentication Login List	Method 1	Method 2	Method 3	Method 4
defaultList	local	undefined	undefined	undefined

show authentication users

User Name Component

admin	System Login
admin	802.1x
guest	System Login
guest	802.1x
default	System Login
default	802.1x

10 IPFIX Configuration

10.1 IPFIX Overview

The FortiSwitch-500 supports Internet Protocol Flow Information eXport (IPFIX). By default, IPFIX is disabled on all switch ports, and no collectors are established for IPFIX data.

10.2 IPFIX Configuration

10.2.1 Configuring IPFIX

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **ipfix collector <ip_address> all** (where <ip_address> is the IP address at which you wish to add an IPFIX collector). This enables IPFIX and sends IPFIX information to the collector from all switch ports. (To export information from only one port, replace **all** with <slot/port> (where <slot/port> is the port from which you wish to export data. Note that on the FortiSwitch-500, the *slot* value is always "1".)

Optional Steps:

3. The default report duration is 15 seconds. If you wish to change the report duration, type **ipfix report-timer <5-60>** (where <5-60> is the desired report duration in seconds).
4. The FortiSwitch-500 sends data traffic to UDP port 2055 by default. If you wish to send traffic to a different port, type **ipfix collector <ip_address> port <0-65535>** (where <ip_address> is the IP address of the IPFIX collector and <0-65535> is the UDP port to which you want to send data traffic).

10.2.2 Viewing IPFIX Information

To display the IPFIX state of switch ports and the IP address and port configuration of IPFIX collectors, type **show ipfix** from Enable Mode.

11 Setting Up Partitions

11.1 Partitioning Overview

The FortiSwitch-500 allows users to configure partitions in the fabric (each partition consisting of a combination of SVLANs) in order to allocate bandwidth to specific traffic types. The switch can distribute traffic to partitions based on a packet's input port and VLAN tag, and each partition can be further divided into four priority classes – default class (0), A, B, and C, based on either the 802.1d or diffserv priority fields. Class A maps to 802.1p priority values 2 and 3, class B to 4 and 5, and class C to 6 and 7.

Note: *in a multi-chassis fabric, partitioning configurations must be made consistently in every switch participating in the fabric.*

11.2 Partition Configuration

11.2.1 Creating Partitions for VLAN Segregation

Partitions may be used to segregate traffic on different VLANs as it passes through the switch by creating partitions that mirror the VLANs themselves. To do this, create a separate partition for each VLAN.

The example below outlines the steps for creating separate partitions for each of four VLANs. In the example, the VLANs are numbered 11-14, and each partition is given the same number as the VLAN which it is created to segregate. This example also assumes that 12 SVLANs have been created on the switch (the default is 6); the 12 SVLANs available on the switch are distributed evenly among the four partitions, and each port is configured to direct incoming traffic to the partition specific to the incoming packet's VLAN tag.

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **fabric-control partition 11 svlan 1001 1002 1003** This creates a new partition with an ID of 11 and assigns SVLANs 1001-1003 to that partition.
3. Type **fabric-control partition 12 svlan 1004 1005 1006** to create partition 12 and assign SVLANs 1004-1006 to it.
4. Type **fabric-control partition 13 svlan 1007 1008 1009**
5. Type **fabric-control partition 14 svlan 1010 1011 1012**
6. Type **port 1/1** to enter Config Port Mode for port 1/1.
7. Type **fabric-control partition 11 vlan 11** This configures the switch to send all traffic entering on port 1/1 and tagged as belonging to VLAN 11 through the switch on partition 11.
8. Type **fabric-control partition 12 vlan 12**
9. Type **fabric-control partition 12 vlan 13**
10. Type **fabric-control partition 12 vlan 14**
11. Type **exit**, then type **port 1/2** to enter Config Port Mode for port 1/2, then repeat steps 7 through 10.

12. Repeat step 11 for each port on the switch.

After this procedure, traffic entering the switch will be segregated by partition according to its VLAN tag; packets tagged VLAN 11 will be routed on partition 11, etc.

11.2.2 Creating Partitions for Priority Segregation

In addition to segregating by VLAN, partitions may also be used to segregate traffic by its IEEE 802.1p or DiffServ priority field.

The example below outlines the steps for creating a partition in which more SVLANs are assigned to higher priority traffic. (Note that the FortiSwitch-500 recognizes three levels of traffic priority: level a (the lowest) maps to 802.1p levels 2 and 3; level b maps to 802.1p levels 4 and 5, and level c (the highest) maps to 802.1p levels 6 and 7.)

1. From Enable Mode, type **config** to enter Config Mode.
2. Type **fabric-control partition 11 priority a svlan 1001 1002** This creates a partition with an ID of 11, and specifies that traffic with the lowest priority level will only be passed on SVLANs 1001 and 1002.
3. Type **fabric-control partition 11 priority b svlan 1001 1002 1003 1004** This adds SVLANs 1003 and 1004 to the pool of available routes for traffic of priority b in partition 11.
4. Type **fabric-control partition 11 priority c svlan 1001 1002 1003 1004 1005 1006** This adds SVLANs 1005 and 1006 to the pool of available routes for traffic of the highest priority (priority c) in partition 11.

11.2.3 Viewing Partition Information

To see a list of all partitions configured on the switch and the SVLANs assigned to each partition, type **show fabric-control partition**. To view information for one partition only, type **show fabric-control partition <1-1000>** where <1-1000> is the ID of the partition about which you would like the information.

12 File Management

12.1 File Management Overview

Each FortiSwitch-500 Ethernet Fabric Switch has two storage locations: the internal disk (specified by **disk** in the CLI) and the external disk (specified by **extdisk** in the CLI). Because the external disk can be easily removed, the configuration file used by the switch at startup is stored on the internal disk. By default, the **copy** command uses the internal disk as both its default source path and its default destination path.

Also please note that as of the date of this publication, the external disk is not yet fully supported.

Almost all file management commands are performed from File Mode. To access File Mode, type **file** in Enable Mode.

12.2 Basic File Operations

12.2.1 Listing the Contents of the Internal Flash Drive

To list the contents of the internal drive, type **dir** from File Mode.

12.2.2 Saving the Running Configuration

If you have made changes to the running configuration since startup, they will be overwritten on reboot unless they are saved to the startup-config file. To save the current configuration to the startup-config file, type **copy running-config startup-config** from File Mode.

12.2.3 Resetting the Configuration to Factory Defaults

To overwrite the startup configuration file with the factory defaults, type **copy default-config startup-config** from File Mode. Resetting the switch will restore the running configuration to factory defaults.

12.2.4 Deleting Files

To delete a file from the internal drive, type **del <file_name>** from File Mode, where **<file_name>** is the name of the file to be deleted.

12.2.5 Transferring Files

Simple file transfers to and from the top directory level of the internal disk can be carried out using FTP or TFTP.

FTP

To transfer files using FTP, establish an FTP session by typing **ftp <ip_address>** from File Mode, where **<ip_address>** is the IP address of the FTP server.

TFTP Uploads

To upload files from the internal drive using TFTP, from File Mode type **tftp put** *<file_name>* *<ip_address>:!<file_path>[/<target_file>]*, where:

- *<file_name>* is the name of the file to be transferred
- *<ip_address>* is the IP address of the TFTP server to which you are uploading the file
- *<file_path>* is the path to the directory to which you are uploading the file
- *[target_file]* is the optional target file name; if none is specified, the name of the source file is used.

TFTP Downloads

To download files to the internal drive using TFTP, from File Mode type **tftp get** *<ip_address>:!<file_path>/<file_name>* *[target_file]*, where:

- *<ip_address>* is the IP address of the TFTP server from which you are downloading the file
- *<file_path>* is the path to the directory from which you are downloading the file
- *<file_name>* is the name of the file to be transferred
- *[target_file]* is the optional target file name; if none is specified, the name of the source file is used.

12.3 System Upgrades

To upgrade the system on the FortiSwitch-500, download the updated system image from the Fortinet support portal and set it as the default system image for the switch following the procedure below.

12.3.1 Upgrading the System

1. **Download image to a local server.** Contact Fortinet Technical Support to download the appropriate system image to a local FTP or TFTP server on your network. Fortinet recommends installing the image onto the switch from a local server on your network to reduce the number of hops in the final installation process and ensure higher data integrity in the image.
2. **Load image onto switch.**

FTP

If using FTP, type the **ftp** command in File Mode to open a connection to the local FTP server onto which you've downloaded the image and copy the image to the switch using standard FTP commands.

TFTP

If using TFTP, use the **tftp get** command to copy the image from the local TFTP server onto which you've downloaded the image as follows:

- a. Access the CLI with admin privileges, and type **enable** to access Enable Mode.
- b. Type **file** to access File Mode.
- c. To load the image from your TFTP server, type **tftp get** *<ip_address>:!<file_path>/<file_name>* *[target_file]* where *<ip_address>:!<file_path>* is the IP address and file path of the local FTP server

location of the new image file, *<file_name>* is the name of the new image and *<target_file>* is the file name on the FortiSwitch-500.

3. **Set system image.** Set the newly downloaded image as the system image by using the **system image** command. From File Mode, type **system image <file_name>** (where *<file_name>* is the name of the new system image) to set the system image for the switch.
4. **Reload system.** Finish the process by resetting the switch.
 - a. From File Mode, type **exit** to access Enable Mode.
 - b. Type **reload** to reset the switch without power cycling. This command terminates all network connections and loads the settings from the startup-config file.