

Open Automation Guide




Configuration and Command Line Reference

July 2013



Force10

Notes, Cautions, and Warnings

-  **NOTE:** A NOTE indicates important information that helps you make better use of your computer.
-  **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
-  **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

© 2013 Dell Networking. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel, Pentium, Xeon, Core™ and Celeron are registered trademarks of Intel Corporation in the U.S. and other countries. AMD is a registered trademark and AMD Opteron™, AMD Phenom™, and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® is a registered trademark and SUSE™ is a trademark of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter®, and vSphere® are registered trademarks or trademarks of VMWare, Inc. in the United States or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

| | | |
|---|---|----|
| 1 | About this Guide | 9 |
| | Objectives | 9 |
| | Audience | 9 |
| | Supported Platforms and Required FTOS Versions | 9 |
| | Conventions | 10 |
| | Information Symbols | 10 |
| | Related Documents | 11 |
| 2 | Open Automation Framework | 13 |
| | Bare Metal Provisioning | 14 |
| | Smart Scripting | 15 |
| | Virtual Server Networking | 15 |
| | Programmatic Interface | 16 |
| | Web Server with HTTP Support | 16 |
| 3 | Bare Metal Provisioning 1.5 | 17 |
| | Auto-configuring Switches | 18 |
| | Prerequisites | 19 |
| | DHCP Server | 19 |
| | TFTP File Server | 20 |
| | DNS Server | 20 |
| | Restrictions | 20 |
| | Reload Progress Messages | 21 |
| | Auto-Configuration Modes | 21 |
| | Factory-Default Mode (Mode A) | 21 |
| | DHCP Configuration | 21 |
| | FTOS Image Retrieval | 22 |
| | Startup Configuration Retrieval | 22 |
| | Factory-Default Mode: Boot and Set-up Behavior | 22 |
| | DHCP-Server Mode (Mode B) | 25 |
| | DHCP Configuration | 26 |
| | FTOS Image Retrieval | 26 |
| | Startup Configuration Retrieval | 26 |
| | DHCP-Server Mode: Boot and Set-up Behavior | 26 |
| | DHCP-Client Mode (Mode C) | 27 |
| | MAC-Based IP Address Assignment | 28 |
| | DHCP-Client Mode Prerequisites | 28 |
| | DHCP-Client Mode: Boot and Set-up Behavior | 29 |
| | DHCP-Client-Only mode (Mode D) | 36 |
| | DHCP Configuration | 38 |
| | FTOS Image Retrieval | 38 |
| | Startup Configuration Retrieval | 38 |
| | DHCP-Client-Only Mode: Boot and Set-up Behavior | 38 |

| | | |
|---|---|----|
| 4 | Bare Metal Provisioning CLI 1.5 | 41 |
| | Overview | 41 |
| | Commands | 41 |
| 5 | Bare Metal Provisioning 3.0 | 47 |
| | Overview | 47 |
| | Prerequisites | 48 |
| | Important Information | 48 |
| | Standard Upgrades with BMP | 48 |
| | BMP Process Overview | 49 |
| | Preparing BMP | 49 |
| | DHCP Server | 50 |
| | DHCP Configuration | 50 |
| | DHCP Server IP Blacklist | 51 |
| | MAC-Based Configuration | 51 |
| | File Server | 52 |
| | Domain Name Server | 52 |
| | Reload Modes | 53 |
| | BMP Mode | 53 |
| | BMP Mode Prerequisites | 53 |
| | MAC-Based IP Address Assignment | 54 |
| | Normal Mode | 54 |
| | DHCP Configuration | 55 |
| | FTOS Image Retrieval | 55 |
| | Scripts | 55 |
| | Preconfiguration Scripts | 55 |
| | Post Configuration Scripts | 56 |
| | Auto-Execution Scripts | 56 |
| | Preconfiguration Process for Scripts | 57 |
| | Configuration Tasks | 57 |
| | System Boot and Set-Up Behavior in BMP Mode | 59 |
| | BMP Mode: Boot and Set-UP Behavior | 61 |
| | Reload Without a DHCP Server Offer | 61 |
| | Reload with a DHCP Server Offer Without an FTOS Offer | 61 |
| | Reload with a DHCP Server Offer and no Configuration File | 62 |
| | Reload with a DHCP Server Offer Without a DNS Server | 63 |
| | Using the Post Configuration Script (BMP Mode Only) | 65 |
| | Reload Using the Auto-Execution Script (Normal Mode Only) | 65 |
| | Script Examples | 66 |
| | Auto-Execution Script - Normal Mode | 66 |
| | Preconfiguration Script - BMP Mode | 69 |
| | Post Configuration Script - BMP Mode | 70 |

| | | |
|---|---|-----|
| 6 | Bare Metal Provisioning (BMP) | 73 |
| | Overview | 73 |
| | Commands | 73 |
| 7 | Smart Scripting | 81 |
| | Overview | 81 |
| | Use Cases | 82 |
| | Downloading the Smart Scripting Package | 83 |
| | Installing Smart Scripting | 84 |
| | Displaying Installed Packages | 85 |
| | Uninstalling Smart Scripting | 86 |
| | Limits on System Usage | 86 |
| | Supported UNIX Utilities | 87 |
| | Creating PERL, Python, and UNIX Scripts | 88 |
| | Creating a User Name and Password for Smart Scripting | 89 |
| | Downloading Scripts to a Switch | 89 |
| | Setting a Search Path for Scripts | 90 |
| | Running Scripts with User Privileges | 90 |
| | Scheduling Time / Event-based Scripts | 91 |
| | Triggering a Script to Run | 91 |
| | Managing Executed Scripts | 92 |
| | Viewing Script Information | 93 |
| | Logging in to a NetBSD UNIX Shell | 93 |
| | Running a Script from the UNIX Shell | 93 |
| | Using the PERL API | 94 |
| | Creating a PERL API Script | 94 |
| | Running a PERL API Script | 97 |
| | Using the Python API | 97 |
| | Creating a Python API Script | 98 |
| | Running a Python API Script | 100 |
| | Using UNIX Shell Scripting | 101 |
| | Creating a UNIX API Script | 101 |
| | Running a UNIX API Script | 103 |
| 8 | Virtual Server Networking | 105 |
| | Overview | 106 |
| | Hypervisor Modes | 107 |
| | VSN Persistency | 107 |
| | VLAN configuration | 107 |
| | Management VLAN | 107 |
| | Data VLANS | 108 |
| | Hypervisor-unaware VLANs | 108 |

| | |
|--|------------|
| Installing VSN | 108 |
| Enabling VSN in a Hypervisor Session | 110 |
| Discovery | 112 |
| Connectivity | 112 |
| Running VSN Scripts | 113 |
| Stopping a Hypervisor Session | 114 |
| Disabling a Session | 114 |
| Removing a Session | 114 |
| Uninstalling VSN | 115 |
| Viewing VSN information | 115 |
| 9 Virtual Server Networking CLI | 119 |
| Overview | 119 |
| Commands | 119 |
| 10 Smart Scripting CLI | 131 |
| Overview | 131 |
| Commands | 131 |
| 11 Programmatic Interface | 147 |
| Overview | 147 |
| Important Points to Remember | 147 |
| Supported Resources | 148 |
| /ftos | 148 |
| /ftos/router | 148 |
| /ftos/router/bgp | 148 |
| bgp-stats | 148 |
| fp-stats | 149 |
| if:interfaces | 149 |
| if-mib | 150 |
| if-mib interfaces | 150 |
| Retrieving IF Index Information | 150 |
| REST Authentication | 151 |
| Configuring a BGP Network Topology | 151 |
| Configure the Physical Interfaces | 152 |
| Review Interface Configurations and Statistics | 154 |
| POST and GET Request Examples | 156 |
| Available Resource Paths | 157 |
| HTTP Status Error Codes | 160 |
| Elements of REST API XML Attributes | 161 |
| Border Gateway Protocol | 162 |
| create | 162 |

| | |
|---|-----|
| delete | 163 |
| 12 Programmatic Interface CLI | 165 |
| Overview | 165 |
| 13 Programmatic Interface REST API Commands | 167 |
| Overview | 167 |
| 14 Web Server with HTTP Support | 171 |
| Web Server | 171 |
| 15 Web Graphical User Interface | 173 |

About this Guide

Objectives

This document describes the components and uses of the Open Automation Framework designed to run on the Dell Networking Operating System (FTOS), including:

- Bare Metal Provisioning (BMP)
- Smart Scripting
- Virtual Server Networking (VSN)
- Programmatic Interface
- Web graphic user interface (GUI) and HTTP Server

Audience

This document is intended for data center managers and network administrators responsible for virtualization or system management. It assumes basic knowledge about virtualization technology and networking.



Note: Although this document contains information on protocols, it is not intended to provide complete information on protocol configuration and usage. For this information, refer to the document listed in [Related Documents](#) and the IETF Requests for Comment (RFCs).

Supported Platforms and Required FTOS Versions

The Open Automation release is supported on the following Dell Networking switches and minimum FTOS versions.

- S55 switches require FTOS version 8.3.5.2 or later.
- S60 switches require FTOS version of 8.3.3.7 or later.
- S4810 switches require FTOS version 8.3.10.1 or later.

- S4820T switches require FTOS version 9.2(0.0) or later.
- Z9000 switches require FTOS version 9.0.0.0 or later. (SmartScripts and SmartUtil support only)
- MXL Switches require FTOS version 9.2(0.0) or later.

Conventions



This document uses the following conventions to describe command syntax:

| Convention | Description |
|------------------|--|
| keyword | Keywords are shown in bold and should be entered in the CLI as listed. |
| <i>parameter</i> | Parameters are shown in italics and require a number or word to be entered in the CLI. |
| {X} | Keywords and parameters within braces are required entries and must be entered in the CLI. |
| [X] | Keywords and parameters within brackets are optional. |
| x y | Keywords and parameters separated by bar require you to choose one. |

Information Symbols

Table 1-1 describes the symbols used in this document.

Table 1-1. Information Symbols

| Symbol | Type | Description |
|---|---------------------------|---|
|  | Note | Informs you about important operational information. |
|  | FTOS Behavior | Informs you about an FTOS behavior. These behaviors are inherent to the Dell Networking system or FTOS feature and are non-configurable. |
| <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">S55</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">S60</div> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-bottom: 5px;">S4810</div> S4820T Z9000 MXL Switch | Platform-specific Feature | <p>Informs you of the platform supporting the Open Automation features.</p> <p>For example, the S55, S60, S4810 and S4820T platforms support all Open Automation features. The Z9000 platform supports the SmartScripts and SmartUtil features. The MXL platform supports Programmatic Interface and the SmartScripts features.</p> |
| | Exception | A note associated with some other text on the page that is marked with an asterisk. |

Related Documents

For more information about the Dell Networking switches discussed in this document, refer to the following documents:

- S55
 - *FTOS Command Line Reference Guide for the S55 System*
 - *FTOS Configuration Guide for the S55 System*
 - *Installing the S55 System*
- S60
 - *FTOS Command Line Reference Guide for the S60 System*
 - *FTOS Configuration Guide for the S60 System*
 - *Installing the S60 System*
- S4810
 - *FTOS Command Line Reference Guide for the S4810 System*
 - *FTOS Configuration Guide for the S4810 System*
 - *Installing the S4810 System*
- S4820T
 - *FTOS Command Line Reference Guide for the S4820T System*
 - *FTOS Configuration Guide for the S4820T System*
 - *Installing the S4820T System*
- Z9000
 - *FTOS Command Line Reference Guide for the Z9000 System*
 - *FTOS Configuration Guide for the Z9000 System*
 - *Installing the Z9000 System*
- MXL Switch
 - *FTOS Command Line Reference Guide for the MXL 10/40GbE Switch IO Module*
 - *FTOS Configuration Guide for the MXL 10/40GbE Switch IO Module*
 - *MXL 10/40GbE Switch IO Module Getting Started Guide*
- [FTOS Release Notes](#) for the platform and version you are using.

Open Automation Framework

Open Automation Framework is supported on platforms: **S60** **S55** **S4810**
S4820T Z9000, MXL

Dell Networking's Open Automation Framework is designed to provide an open, industry standards-based automation technology that simplifies the management of dynamic virtual data centers and reduces risk and overhead.

With the Open Automation Framework, resources in a virtualized data center are managed more flexibly and efficiently without requiring the manual reconfiguration of virtual switches (vSwitches), virtual machines (VMs) on network servers, and VM control software each time there is a change in the network. Automated provisioning of network resources during virtual machine migration ensures that connectivity and security policies are maintained.

Industry-standard scripting languages, such as Perl and Python, are used to automate the monitoring and management of network devices. Virtual resources can be quickly allocated to adapt to configuration changes. Failure of a network device is more quickly detected and resolved. As a result, network uptime increases.

Automated bare metal provisioning allows you to reduce operational overhead by automatically configuring Dell Networking switches, accelerating switch installation, and simplifying operating system upgrades.

Support for multiple, industry-standard hypervisors, virtual switches, and system management tools ensure that automated solutions work within an established data-center environment in which heterogeneous server, storage, and networking equipment interoperate. In addition, Open Automation allows you to customize automated solutions for your current multi-vendor virtualization environment.

An onboard Web-based graphical user interface (GUI) provides a user-friendly way to monitor and manage a data center network. HTTP and HTTPS daemons run on supported switches to provide additional management capability, such as the REST application programming interface (API).

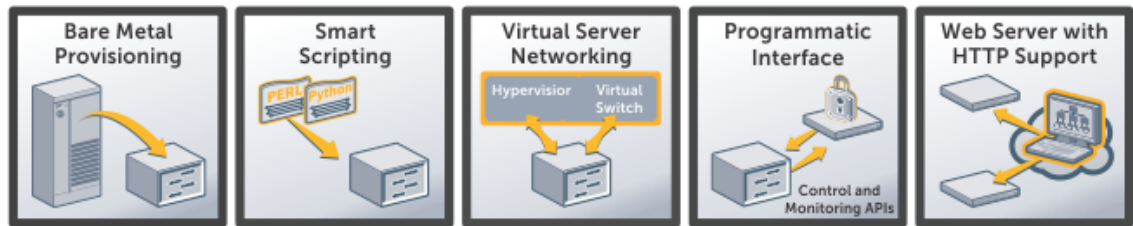
The Open Automation Framework consists of the following network management tools:

- Bare Metal Provisioning
- Smart Scripting
- Virtual Server Networking

- Programmatic Interface
- Web Server with HTTP Support

You can use these components together or independently to extend and add functionality to the FTOS operating system without requiring updates to an FTOS release.

Figure 2-1. Open Automation Framework



Note: The *Open Automation Framework* is referred to as *Open Automation* in the rest of this document.

Bare Metal Provisioning

Bare Metal Provisioning (BMP) provides the following features:

- Automatic network switch configuration and automated configuration updates
- Enforced standard configurations
- Reduced installation time
- Simplified operating system upgrades

Automated bare metal provisioning reduces operational expenses, accelerates switch installation, simplifies upgrades and increases network availability by automatically configuring Dell Networking switches. BMP eliminates the need for a network administrator to manually configure a switch, resulting in faster installation, elimination of configuration errors and enforcement of standard configurations.

With bare metal provisioning, after a switch is installed, the switch searches the network for a DHCP server. The DHCP server provides the switch with an IP address and the location of a file server, such as TFTP. The file server maintains a configuration file and an approved version of FTOS, the operating system for Dell Networking switches. The switch automatically configures itself by loading and installing an embedded FTOS image with the startup configuration file.

For more information on Bare Metal Provisioning, refer to the *FTOS Configuration Guide* for the S55, S60, S4810, S4820T and Z9000 switches or to the *Configuration Guide for the MXL 10/40GbE Switch IO Module* for MXL switches.

Smart Scripting

Smart Scripting provides:

- Support for industry-standard languages, such as Perl and Python, avoiding the need to learn a new proprietary scripting language
- Customization of device monitoring and management to suit your network needs, including custom maintenance tasks, discovery programs, and event logging for faster problem resolution

Smart scripting increases network availability and manageability by allowing network administrators to deploy custom monitoring and management scripts on Dell Networking switches. Using custom scripts, network administrators can implement version control systems, automatically generate alerts, create custom logging tools and automate management of network devices. Any function that can be performed through the FTOS command-line interface (CLI) can be performed with smart scripting.

The scripting environment provided by Smart Scripting (Perl, Python, and UNIX shell scripts) makes it easy for IT administrators to quickly develop scripts without having to learn a new scripting language.

Virtual Server Networking

Virtual Server Networking (VSN) provides:

- Automatic re-provisioning of VLANs when you migrate virtual machines (VMs).
- Support for multiple hypervisors, such as VMware and Citrix XenServer.

Virtual data centers require network infrastructure to be dynamic to ensure that network connectivity and QoS and security policies are maintained when VMs are migrated. VSN facilitates communication between Dell Networking switches and VM management software to automatically re-provision VMs and associated VLANs during virtual machine migration.

As a result, VSN greatly simplifies many of the tasks associated with virtualized computing environments. Network administrators can manage the network while server administrators manage the servers. No manual VLAN reconfiguration is required when you migrate VMs.

VSN software supports the following hypervisors:

- VMware vSphere 4.0/4.1/5.0
- Citrix XenServer 5.6/6.0

Programmatic Interface

Programmatic Interface provides application programming interfaces (APIs) that allow FTOS switches to be managed by in-house or third-party system management tools.

- Common third-party management tool sets are supported as plug-ins to the Open Automation Framework, including Dell AIM, EMC Smarts Ionix, IBM Systems Director, HP Network Automation (NA), CA Spectrum Infrastructure Manager, and Oracle Enterprise Manager (OEM).
- Industry-standard management protocols are supported, such as SNMP (Get and Set) and REpresentational State Transfer (REST).
- User protocols are supported, such as CLI/CLI-script, XML (Get and Set) and Web-based commands.

Programmatic Interface greatly improves network manageability by allowing Dell Networking switches to be managed by third-party system management tools via standard program interfaces.

The programmatic management environment and set of interfaces communicate directly with third-party system management tools, avoiding the need for a dedicated network management tool. As a result, network management is simplified and the number of management tools is minimized.

Web Server with HTTP Support

The Open Automation Framework supports Web connectivity through its Web server with HTTP support.

- The Web Server consists of both HTTP and HTTPS daemons running on a switch.

Bare Metal Provisioning 1.5

Bare Metal Provisioning version 1.5 is supported on the [S55](#) [S60](#) platforms and is included as part of the FTOS image.

For information on how Bare Metal Provisioning version 3.0 is supported on the S4810, S4820T, and Z9000 platforms, refer to [Chapter 5, Bare Metal Provisioning 3.0](#).

Bare Metal Provisioning (BMP) minimizes the effort required to manage increasing numbers of network devices in a data center by:

- Automatically configuring switches, including stacked switches
- Ensuring standard configurations across installed devices
- Automating configuration updates

Pre-defined configurations are stored in a configuration management database and automatically loaded onto supported Dell Networking switches through DHCP, providing the following benefits:

- Lower network complexity—Network administrators can ensure that data center switches are configured in a consistent manner.
- Reduced installation time—Less time is required to install and configure switches by searching the network for a valid configuration file and an approved version of the FTOS operating system.
- Policy-based configuration management—Network administrators can define a network configuration based on policy and use BMP to ensure that every network switch is configured accordingly.

BMP automates the following configuration steps on a supported Dell Networking switch:

- Obtain an IP address, configuration, and boot image information from a DHCP server.

You can also access a switch through an Ethernet management port with or without DHCP-based, dynamic IP address configuration of the device.

- Boot up in Layer 2 mode with interfaces already in **no shutdown** mode and some basic protocols enabled to protect the system and the network.



Note: If the network has VLT enabled on aggregator switches and you are configuring the ToR to load using BMP, ensure the aggregator switches are configured with the **lACP ungroup member-independent vlt** CLI if the DHCP/TFTP server is reachable via the interface configured as part of VLT lag.

Auto-configuring Switches

Bare Metal Provisioning provides various ways (modes) in which a switch can be automatically configured when it boots up.

By default, at initial power-up, a Dell Networking switch running BMP boots up in an auto-configuration mode called DHCP-Client mode (auto-configuration mode C below). When the system boots up, it connects to a DHCP server on which the required FTOS image and startup configuration files are stored. These files are downloaded to the system and the system reloads with these images. Each switch has its own startup configuration file on the DHCP server and automatically connects to the management network (when configured).

The auto-configuration mode used to boot up a switch remains in the non-volatile memory. When an auto-configured reload is performed, the switch boots up in the mode stored in non-volatile memory.

Using BMP, you can configure a switch to reload in the auto-configuration modes described below. The new mode is retained in non-volatile memory. To display the current auto-configuration mode, enter the **show system brief** command.

Figure 3-1. Displaying Auto-Configuration Mode: show system brief

```
FTOS# show system brief
Stack MAC : 00:01:e8:82:09:b0
Reload Type : normal-reload
```

BMP 1.5 supports the following auto-configuration modes to reload a switch:

- **Factory-Default switch (Mode A):** A switch boots up with the factory-default FTOS image and startup configuration to permit a local installer to connect a PC to its management port (or other port) to configure the switch or stack. The system has a temporary IP address.
- **DHCP-Server mode (Mode B):** The switch loads the FTOS image from flash memory with the factory-default configuration and acts as DHCP server with a temporary management IP address, allowing connectivity to a user device to configure the startup configuration.

- **DHCP-Client mode (Mode C):** Default auto-configuration mode on a new switch that arrives from Dell Networking. The system loads without using the startup configuration in flash memory and connects to a DHCP server where the required FTOS and configuration files are stored. These files are downloaded to the switch, which reloads with these images. If no DHCP server responds, the system reloads in factory-default mode A.
- **DHCP-Client-Only mode (Mode D):** The system loads for a specified number of retries without using the startup configuration in flash memory and connects to a DHCP server where the required FTOS and configuration files are stored. These files are downloaded to the system and the system is reloaded with these images. If no DHCP server responds after the configured number of retries, the system reloads in factory-default mode A.

Default BMP mode: DHCP-Client mode (Mode C)

Normal reload mode: After a switch boots up in an auto-configuration mode, you can reconfigure it to ignore the currently configured mode by entering the **reload** command and boot up in the future in normal reload mode. In Normal mode, the system loads the FTOS image and startup configuration file in the local flash. New configurations require the management IP and management interface IP addresses to be configured manually. Note that you can always manually force a switch to boot up in normal mode by entering the **reload** command; no additional parameters are required.

To reconfigure a switch to ignore the current auto-configuration mode and reload in normal mode, enter the **reload** command.

| Command Syntax | Command Mode | Purpose |
|----------------|----------------|--|
| reload | EXEC Privilege | Reload the system using the FTOS image and startup configuration file stored in the local flash. |

Prerequisites

Before you use BMP 1.5 to auto-configure a supported Dell Networking switch, you must first configure a DHCP, DNS, and file server in the network.

DHCP Server



Note: The factory-default switch (Mode A) and DHCP-server (Mode B) auto-configuration modes do not require a DHCP server.

You must first configure a DHCP server before you can use DHCP-Client and DHCP-Client-Only auto-configuration mode on a switch. Configure the DHCP server with the set of parameters described below for each client switch. Refer to the *FTOS Configuration Guide: Dynamic Host Configuration Protocol* chapter for detailed information.

Although an IP address is the only required setting, Dell Networking recommends that you configure all of the following parameters for easier use.

- Image name— FTOS image to be loaded on a switch.
- Configuration file—Configuration to be applied to a switch.
- File server IP address—File server where the FTOS image and configurations file are stored.
- Domain name server— DNS server to be contacted to resolve the host name.
- IP address—Dynamic IP address assigned by the DHCP server.

TFTP File Server

In BMP 1.5, you must configure a TFTP file server as the network source from which a switch retrieves the FTOS image file to be loaded and the startup configuration file to be applied. On a TFTP server, the required files are commonly found in the `/tftpboot` directory.



Note: In BMP 2.0, other types of file servers are supported.

DNS Server

You must configure a domain name server (DNS) to determine the host name applied in the switch startup configuration when no configuration file is retrieved from the DHCP server. The DNS server is contacted only when no configuration file is contained in a DHCP server response and the host name is not resolved from the `network-config` file on the switch.

Restrictions

BMP 1.5 is not supported on the user ports of a switch. BMP 1.5 is supported only on management ports.

Reload Progress Messages

A supported Dell Networking switch displays the system boot status on the console as a reload is progressing. The progress messages describe connections to network servers, assigned IP addresses and gateways, and the success or failure of these connections.

Auto-Configuration Modes

You can configure a supported Dell Networking switch to boot up in the following auto-configuration modes:

- [Factory-Default Mode \(Mode A\)](#)
- [DHCP-Server Mode \(Mode B\)](#)
- [DHCP-Client Mode \(Mode C\)](#)
- [DHCP-Client-Only mode \(Mode D\)](#)

Default: The DHCP-Client auto-configuration mode is the boot mode configured by default for BMP 1.5 on a new system arriving from Dell Networking.

Factory-Default Mode (Mode A)

When reloaded in factory-default mode, the switch boots up with the factory-default settings (FTOS image and startup configuration file in the local flash) applied to the system. The management port is configured with the temporary static IP address 192.168.0.1. You can connect to the management port with an IP address on the same network, and log in to the system through a telnet or SSH session.

You can replace the temporary management IP address with a user-configured management IP address. The IP address 192.168.0.1 is active for ten minutes. After ten minutes, a user-configured IP address is applied to the management interface.

To configure a switch to reload using auto-configuration mode A, enter the **reload factory-default** command.

| Command Syntax | Command Mode | Purpose |
|-------------------------------|----------------|--|
| reload factory-default | EXEC Privilege | Reload the system with a temporary IP address using the FTOS image and startup configuration file stored in the local flash. |

DHCP Configuration

Mode A does not require a separate DHCP server configuration.

FTOS Image Retrieval

The FTOS image is loaded from the local flash.

Startup Configuration Retrieval

The startup configuration file is loaded from the local flash. [Figure 3-2](#) shows an example of how a switch is reloaded using factory-default settings.

Figure 3-2. Factory-Default Startup Configuration Settings

```

interface range GigabitEthernet 0/0 - 47      Interfaces boot up in:
  no shutdown <----- no shutdown mode
  switchport <----- Layer 2 mode
!
interface range TenGigabitEthernet 0/48 - 51
  no shutdown
  switchport
!
interface ManagementEthernet 0/0
  ip address 192.168.0.1/24 <----- Temporary management IP address
  no shutdown
!
ip telnet server enable
!
ip ssh server enable
!
protocol spanning-tree rstp
  no disable
!
protocol lldp
  no disable
  advertise dot1-tlv port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-description   system-name
  advertise med
no disable
!
end

```

Factory-Default Mode: Boot and Set-up Behavior

After a switch boots up, use the **show users** command to view the IP addresses configured for connecting devices and the status of each connection; for example:

Figure 3-3. Displaying Connected Devices After Bootup

```
FTOS00:26:15: %STKUNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
on vty0 (192.168.0.5)
FTOS#00:26:19: %STKUNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
on vty1 (192.168.0.5)

FTOS#show users
      Line           User           Host(s)      Location
*    0 console 0
      2 vty 0
      3 vty 1
      idle
      idle      192.168.0.5
      idle      192.168.0.5
```

During the first ten minutes after authentication is enabled on the switch, access to the system is not secured. No password is required as shown in [Figure 3-4](#).

Figure 3-4. Accessing a Switch During the First Ten Minutes after Bootup: No Password Required

```
[root@localhost tftpboot]# telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1 (192.168.0.1).
Escape character is '^]'.
FTOS>enable
FTOS#configure
FTOS(conf)#hostname customer
customer(conf)#exit
customer#exit
Connection closed by foreign host.
[root@localhost tftpboot]#

[root@localhost etc]# ssh 192.168.0.1

FTOS>
FTOS>enable
FTOS#configure
customer(conf)#hostname FTOS
FTOS(conf)#exit
FTOS#exit
Connection to 192.168.0.1 closed by remote host

Connection to 192.168.0.1 closed.
```

After the initial unsecured ten minutes, you are prompted for a password to log on to the system. To ensure system access and authentication, configure user names and password as described in the *FTOS Configuration Guides*.

Dell Networking strongly recommends that you reconfigure the temporary management IP address (192.168.0.1) within ten minutes after a switch boots up in factory-default mode. The user-configured management IP address takes effect after the ten-minute period expires.

Following the ten-minute period, after authentication is enabled, you can remotely access the switch using telnet or SSH as shown in [Figure 3-5](#).

Figure 3-5. Accessing a Switch After the First Ten Minutes after Bootup

```
[root@localhost tftpboot]# telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.4 (192.168.0.1).
Escape character is '^'.
Login: user1
Password:
FTOS>enable
Password:
FTOS#configure
% Warning: The following users are currently configuring the system:
User "" on line console0
FTOS(conf)#hostname customer
customer(conf)#exit
customer#exit
Connection closed by foreign host.
[root@localhost tftpboot]#

[root@localhost etc]# ssh user@192.168.0.4
user@192.168.0.4's password:
user>enable
Password:
customer#configure
% Warning: The following users are currently configuring the system:
User "" on line console0
customer(conf)#hostname Force10
FTOS(conf)#exit
FTOS#exit
Connection to 192.168.0.4 closed by remote host.
Connection to 192.168.0.4 closed.
[root@localhost etc]#
```

After you change the temporary management IP address 192.168.0.1, the new management IP address is applied to the management interface only after ten minutes from when the change is entered. During this ten minute period, you can still connect to the management port using the IP address 192.168.0.1 as shown in [Figure 3-6](#).

Figure 3-6. Factory-Default Mode: Connecting to the Management Port

```
FTOS(conf)#interface management 2/0
FTOS(conf-if-ma-1/0)#show config
!
interface ManagementEthernet 2/0
  ip address 192.168.0.1/24 <----- Default temporary IP address
  no shutdown
FTOS(conf-if-ma-2/0)#ip address 10.16.149.222/16
00:03:33: %STKUNIT2-M:CP %IFMGR-5-DEFAULT_IP_CHANGE: The management ip
10.16.149.222/16 is changed only in config and it will take effect after 10
minutes

... After ten minutes

FTOS(conf-if-ma-2/0)#show config
!
interface ManagementEthernet 2/0
  ip address 10.16.149.222/16 <----- User-configured IP address
  ip address 192.168.0.1/24 secondary
  no shutdown
FTOS(conf-if-ma-2/0)#00:04:03: %STKUNIT2-M:CP %IFMGR-5-USER_CFG_IP_RESTORED:
The management ip 10.16.149.222/16 is added after the 10 minutes timeout

FTOS(conf-if-ma-2/0)#show config
!
interface ManagementEthernet 2/0
  ip address 10.16.149.222/16
  no shutdown
```

DHCP-Server Mode (Mode B)

In DHCP-Server mode, a switch reloads with the factory-default settings (see [Figure 3-2](#)). A temporary IP address (192.168.0.1) is assigned to the IP management interface and DHCP server capabilities are enabled on the system, so that the system acts as a DHCP server. You can connect to the management port from an IP address on the same network, and log in to the system through telnet or SSH.

A switch that reloads in DHCP-Server mode has the DHCP server configuration shown in [Figure 3-7](#).

Figure 3-7. DHCP Server Configuration in Auto-Configuration Mode B

```
ip dhcp server
!
pool dhcpServer
  network 192.168.0.0/24
  no disable
```



Note: DHCP-Server mode is similar to factory-default mode with a DHCP-server configuration enabled. A switch that reloads in DHCP-Server mode has the same startup configuration as in the factory-default mode. In addition, the switch has the DHCP server configuration shown in [Figure 3-7](#).

To configure a switch to reload using auto-configuration mode B, enter the **reload factory-default dhcp-server-mode** command.

| Command Syntax | Command Mode | Purpose |
|--|----------------|--|
| reload factory-default dhcp-server-mode | EXEC Privilege | Reload the system as a DHCP server using the FTOS image and startup configuration file stored in the local flash. You can configure a permanent management IP address and host name. |

DHCP Configuration

Mode B does not require a separate DHCP server configuration.

FTOS Image Retrieval

The FTOS image is loaded from the local flash.

Startup Configuration Retrieval

The default configuration file is loaded from the local flash as in auto-configuration mode A (see [Figure 3-2](#)) with a DHCP configuration so that the system acts as a DHCP server. You can then connect to the switch and manually configure it from another network device using telnet or SSH.

DHCP-Server Mode: Boot and Set-up Behavior

After a switch boots up, enter the **show users** command to view the IP addresses configured for connecting devices and the status of each connection. You can display a list of connected users in the same way as when booting up in factory-default mode (mode A); see [Figure 3-3](#) for an example.

During the first ten minutes after authentication is enabled, access to the system is not secured and no password is required to log in as shown in [Figure 3-4](#).

Dell Networking strongly recommends that you reconfigure the temporary management IP address (192.168.0.1) within ten minutes after a switch boots up in DHCP-Server mode. The user-configured management IP address takes effect after the ten-minute period expires.

Following the ten-minute period, after authentication is enabled, you can remotely access the switch using telnet or SSH as shown in [Figure 3-5](#).

After you change the temporary management IP address 192.168.0.1, the new management IP address is applied to the management interface only after ten minutes from when the change is entered. During this ten minute period, you can still connect to the management port using the IP address 192.168.0.1 as shown in [Figure 3-6](#).

DHCP-Client Mode (Mode C)

The DHCP-Client auto-configuration mode is the boot mode configured by default for BMP on a new system arriving from Dell Networking. Mode C downloads an FTOS image and configuration file from a TFTP server.

When you configure a switch to reload using auto-configuration mode C, the **honor-startup-config** option determines whether the configuration file is retrieved from the startup configuration file stored in the local flash or from a network source, such as a TFTP server. When a switch boots up with this option configured and no startup configuration file is found in the system's flash memory, the following message is displayed:

```
No startup-config file found in flash. This would result in jump start
config being applied.Do you want to proceed [confirm yes/no]:
```

Enter **yes** to retrieve the configuration from a file server; enter **no** to apply the factory-default configuration ([Figure 3-2](#)) to the system.

You must set up a DHCP server and a TFTP server before using auto-configuration mode C. The required FTOS image and configuration files must be stored on the file server in order for the system to download them. A DNS Server is not required for mode C, but is recommended. See [DHCP-Client Mode Prerequisites](#) for more information.

To configure a switch to reload using auto-configuration mode C, enter the **reload factory-default dhcp-client-mode** command. If no startup configuration file is found in flash memory, enter **yes** when prompted to ignore the startup configuration and download the configuration from the file server.

| Command Syntax | Command Mode | Purpose |
|--|----------------|---|
| reload factory-default dhcp-client-mode [honor-startup-config] | EXEC Privilege | Reload the system as a DHCP client. If the honor-startup-config option is set, the startup configuration file stored in the local flash memory is loaded. If the option is not set, the customer.conf configuration file is downloaded from the configured file server. |

MAC-Based IP Address Assignment

One way to deploy the DHCP-Client auto-configuration mode is to configure the DHCP server to assign a fixed IP address and configuration file based on the system's MAC address. In this way, the same IP address is assigned and the same configuration file is retrieved when the switch reloads.

Using a dynamic IP address assignment may create a situation in which the desired configuration is not loaded on the system because the IP address changes each time the system is reloaded.

For example, on a DHCP3 server, you can configure the assignment of a fixed MAC-based IP address and configuration file by entering the following lines of configuration parameters in the **dhcpd.conf** file on the server:

```
host S4810 {
hardware ethernet 00:01:e8:81:e2:39;
fixed-address 20.0.0.48;
option configfile "customer.conf";
}
```

DHCP-Client Mode Prerequisites

Before you use the DHCP-Client mode to auto-configure a switch, you must first configure a DHCP, DNS, and file server in the network.

- Set up a DHCP server. Refer to the *FTOS Configuration Guide: Dynamic Host Configuration Protocol* chapter for detailed information. You must configure the DHCP server to assign an IP address to each system along with the following DHCP server parameters:
 - IP address pool: IP address for the system
 - Image name: FTOS image used to boot up the system
 - Configuration file: Startup configuration parameters to be applied to the system
 - IP address of TFTP file server: File server from which the image and startup configuration file are downloaded.
 - Domain Name server: DNS server to be contacted to resolve the host name

Use the following DHCP option codes in the **dhcpd.conf** file:

- 6: IP address of Domain Name Server, if a DNS server is needed to resolve the IP address of a file server hostname
- 150: IP address of a TFTP server
- 209: Configuration file

For example, a sample **dhcpd.conf** file on a DHCP3 server is as follows:

```
lease-file-name "/var/lib/dhcpd/dhcpd.leases";
option configfile code 209 = text;
option tftp-server-address code 150 = ip-address;
subnet 20.0.0.0 netmask 255.255.255.0 {
    range 20.0.0.26 20.0.0.28;
    filename "FTOS-SC-1-2-0-363.bin";
    option configfile "customer.conf";
    option tftp-server-address 20.0.0.1;
    option domain-name-servers 20.0.0.1;
}
```

- Set up a TFTP server and ensure connectivity.

In BMP 1.5, you must configure a TFTP file server as the network source from which the switch downloads the image file and the configuration file to be applied to the system. On a TFTP server, the required files are commonly stored in the **/tftpboot** directory.

When loading the FTOS image, if the FTOS image on the file server is different from the image stored in local flash memory, the system downloads the image on the file server into the local flash and reboots using that image. If the image is the same, the system reloads from the local flash without downloading a new image.

- Set up a DNS server. Refer to the *FTOS Configuration Guide: IPv4 Addressing* chapter: *Resolution of Host Names* section for information.

Configure the DNS server to determine a system's host name and the correct configuration file to be downloaded on the system if the DHCP server response does not specify a configuration file and the host name is not resolved using the **network-config** file.

DHCP-Client Mode: Boot and Set-up Behavior

When a switch that is configured to reload in DHCP-Client mode boots up, one of the following scenarios may occur:

- [Reload without a DHCP Server offer](#)
- [Reload with a DHCP Server offer without an FTOS image](#)
- [Reload with a DHCP Server offer without a File Server Address](#)
- [Reload with a DHCP Server offer without a Configuration File](#)
- [Reload with a DHCP Server offer without a DNS Server](#)

Reload without a DHCP Server offer

A switch configured to reload in DHCP-Client mode makes one attempt to contact a DHCP server when booting. If a DHCP server cannot be reached, the system falls back to factory-default mode to receive a DHCP offer as follows:

1. The system boots up with the BMP application.

```
Entering Jumpstart app:
Initializing runtime directories
Reading Release Image at 0x40000 Part: A
```

2. The system falls back to factory-default mode when no DHCP offer is received.

```
DHCP offer not received on first try. Exiting. interval 14ry
Switching from dhcp-client-mode to factory-default-mode!
```

3. The system loads the FTOS image from flash memory.
4. The system applies the factory-default configuration (Figure 3-2) without assigning an IP address to the management interface.
5. You must manually configure a management IP address.

Reload with a DHCP Server offer without an FTOS image

If a switch that is configured to reload in DHCP-Client mode reaches a DHCP server but does not locate a downloadable FTOS image file on the server, the FTOS image stored in the local flash is loaded as follows:

1. The system boots up with the BMP application.

```
Entering Jumpstart app:
Initializing runtime directories
Reading Release Image at 0x40000 Part: A
```

2. The system receives a DHCP offer from a DHCP server with the following parameters.

```
***** DHCP OFFER DETAILS *****
DHCP acquired IP           = 20.0.0.77
subnet-mask                = 255.255.255.0
DHCP provided Image file  = NIL
DHCP provided Config file = customer.conf
DHCP Server IP            = 20.0.0.1
TFTP Server IP            = 20.0.0.1
DNS IP                     = 20.0.0.1
*****
```

3. One of the following actions is taken:

- a The system does not receive an FTOS image name in the DHCP server response and no image is downloaded from the file server. The following message appears:

```
DHCP offer does not have Image file name
```

The system boots up with the image stored in the local flash and applies the startup configuration file in the flash.

- b The system receives an FTOS image name in the DHCP server response and downloads the **customer.conf** configuration file from the file-server address if you did not enter the **honor startup-config** option with the **reload**

factory-default dhcp-client-mode command:

```
dhcp.conf
tftping dhcp.conf ...
tftp> Received 119 bytes in 0.0 seconds

tftp success
Re-try count: 1
SUCCEED
customer.conf downloaded
```

4. If the local startup-configuration was applied, manually configure the management IP address using the **interface managementethernet** command.



Note: The IP address assigned by the DHCP server is released at the end of the system reload. The switch attempts to reach the file server four times before sending an error message and proceeding to the next step.

Reload with a DHCP Server offer without a File Server Address

If a switch that is configured to reload in DHCP-Client mode reaches a DHCP server but is not able to reach a file server, the FTOS image stored in the local flash is loaded and the factory-default configuration ([Figure 3-2](#)) is applied as follows:

1. The system boots up with the BMP application.

```
Entering Jumpstart app:
Initializing runtime directories
Reading Release Image at 0x40000 Part: A
```

2. The system receives a DHCP offer from a DHCP server with the following parameters.

```
***** DHCP OFFER DETAILS *****
DHCP acquired IP           = 20.0.0.77
subnet-mask                 = 255.255.255.0
DHCP provided Image file   = FTOS-SC-1-2-0-385.bin
DHCP provided Config file  = customer.conf
DHCP Server IP             = 20.0.0.1
TFTP Server IP             = NIL
DNS IP                      = 20.0.0.1
*****
```

The system does not receive the IP address of a file server from which it can retrieve the FTOS image and configuration file.

3. The system boots up with the image stored in the local flash memory.
4. If the **honor startup-config** option is configured with the **reload factory-default dhcp-client-mode** command, the system applies the startup configuration file from the local flash, otherwise the factory-default settings ([Figure 3-2](#)) are applied.



Note: The IP address assigned by the DHCP server is released at the end of the system reload. The switch attempts to reach the file server four times before sending an error message and proceeding to the next step.

Reload with a DHCP Server offer without a Configuration File

If a switch that is configured to reload in DHCP-Client mode reaches a DHCP server but cannot retrieve a configuration file, the switch looks for a configuration file on the file server *only* if the **honor startup-config** option was not entered with the **reload factory-default dhcp-client-mode** command.

1. The system boots up with the BMP application.

```
Entering Jumpstart app:
Initializing runtime directories
Reading Release Image at 0x40000 Part: A
```

2. The system receives a DHCP offer from a DHCP server with the following parameters.

```
***** DHCP OFFER DETAILS *****
DHCP acquired IP           = 20.0.0.77
subnet-mask                = 255.255.255.0
DHCP provided Image file   = FTOS-SC-1-2-0-385.bin
DHCP provided Config file  = NIL
DHCP Server IP             = 20.0.0.1
TFTP Server IP             = 20.0.0.1
DNS IP                     = 20.0.0.1
*****
```

3. The system downloads the image from the file server.

```
get FTOS-SC-8.3.3.4.bin/server/home/image/FTOS-S60_BM
tftp> Received 21752859 bytes in 17.0 seconds
```

4. The system compares the current local image to the downloaded image as follows:
 - a. If the image versions are same the system loads the FTOS image from the local flash, and does not upgrade with the downloaded image.

```
DOWNLOADED RELEASE HEADER :
Release Image Major Version : 1
Release Image Minor Version : 2
Release Image Main Version  : 0
Release Image Patch Version : 385
```

```
FLASH RELEASE HEADER :
Release Image Major Version : 1
Release Image Minor Version : 2
Release Image Main Version  : 0
Release Image Patch Version : 385
```

The image found in tftp is same

- b If the image versions are different, the system stores the downloaded image in the local flash and loads the image from the flash. This process is repeated until the image versions are the same.

```
DOWNLOADED RELEASE HEADER :  
Release Image Major Version : 8  
Release Image Minor Version : 3  
Release Image Main Version : 3  
Release Image Patch Version : 36
```

```
FLASH RELEASE HEADER :  
Release Image Major Version : 1  
Release Image Minor Version : 2  
Release Image Main Version : 0  
Release Image Patch Version : 385
```

The image found in tftp is different

Erasing Sseries Primary Image, please wait

5. The system looks for the configuration file on the file server. If no configuration file is found, the system tries to locate the configuration file as follows:
 - a Determine the system's host name from the **network-config** file stored on the TFTP server.

When the configuration file provided in the DHCP offer is not present in the file server, the system looks for the **network-config** file which contains the IP-to-host-name mapping. The system determines the *hostname* and then tries to download the *hostname.conf* file from the TFTP server.

If this download is successful, the system applies the configuration from the downloaded file and the host name is applied to the system.

```
network-config
tftping network-config ...
tftp> Received 56 bytes in 0.0 seconds

tftp success
Re-try count: 1
network-config downloaded           In the network.config file, the
customer.conf <----- hostname.conf file is resolved as
tftping customer.conf ...             "customer.config".
tftp> Received 134 bytes in 0.0 seconds

tftp success
Re-try count: 1
SUCCEED
customer.conf downloaded
```

- b Determine the system's host name from the DNS server.

If Step 5a does not succeed, the system tries to determine its *hostname* from the DNS server, and then download the *hostname.conf* file from the TFTP server.

If this is successful, the system applies the configuration from the downloaded file and the hostname is applied to the system.

```
Found hostname as customer from DNS response
customer.conf
tftping customer.conf ...
tftp> Received 77 bytes in 0.0 seconds
```

- c Apply the switch configuration file from the **router.conf** file.

If Step 5b does not succeed, the system tries to download the **router.conf** file from the TFTP server and apply it to the system. The **router.conf** file is a common file stored on a TFTP server.

```
router.conf
tftping router.conf ...
tftp> Received 77 bytes in 0.0 seconds
When all the attempts for the configuration file fails the chassis
applies factory default settings.
*****
Downloading Config file..
DHCP provided Config file : NIL
DHCP Server IP           : 20.0.0.1
DNS Server IP           : 20.0.0.1
DHCP acquired IP        : 20.0.0.47
TFTP Server IP          : 20.0.0.1
*****
network-config
tftping network-config ...

tftp failed
tftping network-config ...

tftp failed
tftping network-config ...

tftp failed
Exceeded re-try limit.
Re-try count: 4
Found hostname as customer from DNS response
customer.conf
tftping customer.conf ...

tftp failed
tftping customer.conf ...

tftp failed
tftping customer.conf ...

tftp failed
Exceeded re-try limit.
Re-try count: 4
router.conf
tftping router.conf ...

tftp failed
tftping router.conf ...

tftp failed
tftping router.conf ...

tftp failed
Exceeded re-try limit.
Re-try count: 4
```



Note: The IP address assigned by the DHCP server is released at the end of the system reload. The switch attempts to reach the file server four times before sending an error message and proceeding to the next step.

Reload with a DHCP Server offer without a DNS Server

Although the DNS server is optional, it allows you to specify the configuration file to be applied to a switch by assigning a hostname.

When the DHCP offer is received and no DNS IP address is specified, if the configuration file cannot be retrieved from a file server:

- The **router.conf** file is applied.
- The factory-default configuration is applied if the **router.conf** file is not found on the file server.



Note: The IP address assigned by the DHCP server is released at the end of the system reload. The switch attempts to reach the file server four times before sending an error message and proceeding to the next step.

DHCP-Client-Only mode (Mode D)

DHCP-Client-Only auto-configuration mode (Mode D) works similarly to DHCP-Client mode (Mode C) with the addition of a specified number of discovery attempts (retries). Mode D boots up a new system with a specified FTOS image and a startup configuration file. Mode D requires the DHCP and file servers to be already configured and contain the desired FTOS image and startup configuration file.

To configure a switch to reload using auto-configuration mode D, enter the **reload factory-default dhcp-client-only-mode** command. If no startup configuration file is found in flash memory, enter **yes** when prompted to ignore the startup configuration and download the configuration from the file server.

| Command Syntax | Command Mode | Purpose |
|---|----------------|---|
| reload factory-default dhcp-client-only-mode [retries] [honor-startup-config] | EXEC Privilege | Reload the system in DHCP client mode and attempt to contact the DHCP server for the FTOS image and configuration file. If the honor-startup-config option is set, the startup configuration file stored in the local flash memory is loaded. |

Use the *retries* option to configure the number of attempts the system makes to reach the DHCP server. If the system cannot reach the DHCP server within the specified number of attempts, it reverts to factory-default auto-configuration mode (Mode A) and waits to be locally configured. By default, the system will attempt an endless number of retries to reach the DHCP server.

Enter the **honor startup-config** option to load the startup configuration file stored in the local flash memory. If the option is not set, the configuration file is downloaded from the configured TFTP server. If you enter this option and no startup configuration is stored in flash memory, the following warning message appears:

```
No startup-config file found in flash. This would result in jump start
config being applied.Do you want to proceed [confirm yes/no]:
```

Enter **yes** to retrieve the configuration from a TFTP server in the network; enter **no** to apply the factory-default configuration ([Figure 3-2](#)) to the system.

DHCP Configuration

Before you configure a switch to auto-configure in Mode D, ensure that you have:

- Set up a DHCP server. Refer to the *FTOS Configuration Guide: Dynamic Host Configuration Protocol* chapter for information.
- Set up a TFTP server and ensure connectivity.
- Set up a DNS server. Refer to the *FTOS Configuration Guide: IPv4 Addressing* chapter: *Resolution of Host Names* section for information.



Note: Do not use the DHCP-Client-Only auto-configuration mode unless you have a DHCP, DNS, and TFTP server already configured. If the servers are not configured and a retry number is not set, the system will endlessly continue discovery attempts and not complete the system reload. Contact the Dell Networking Technical Assistance Center for help getting out of the boot loop.

FTOS Image Retrieval

When loading the FTOS image, if the FTOS image on the TFTP server is different from the image in the local flash, the system downloads the image from the server into the local flash and reloads using the downloaded image.

If the image is the same, the system boots up using the image stored in the local flash without downloading a new image.

Startup Configuration Retrieval

When booting up, the switch determines if the **honor-startup-config** option is configured with the **reload factory-default dhcp-client-only-mode** command. This option reloads the switch using the startup configuration file in the local flash and does *not* download the configuration file from the TFTP server.

By default, when the **honor startup-config** option is not entered with the **reload factory-default dhcp-client-only-mode** command, the switch reloads using the configuration file stored on a TFTP server. The switch retrieves the configuration file according to the hostname-specific file name (for example, system33.config for hostname system33). The system executes the configuration file from the TFTP server, but does not store a copy.

DHCP-Client-Only Mode: Boot and Set-up Behavior

Reload with DHCP Offer

When the switch is configured to reload in DHCP-Client-Only mode with a DHCP server configured, the switch receives a DHCP offer and boot ups in the same way as in DHCP-Client mode (see [DHCP-Client Mode \(Mode C\)](#)).

Reload without DHCP Offer and without Specified Number of Retries

When a switch that is reloading in DHCP-Client-Only mode cannot reach a DHCP server and *does not* have a number of retries configured in the **reload factory-default dhcp-client-only-mode** command, the switch attempts to reach the DHCP server an infinite number of times; for example:

```
Entering Jumpstart app:
  Initializing runtime directories
Reading Release Image at 0x40000 Part: A
add net 0.0.0.0: gateway 0.0.0.0
Unable to obtain a lease on first try. Exiting. interval 16ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 35ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 12ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 69ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 10ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 20ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 83ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 18ry
  Sending DHCP request
.
.
.
```

Reload without DHCP Offer and with Specified Number of Retries

When a switch that is reloading in DHCP-Client-Only mode cannot reach a DHCP server but *does* have a number of retries configured in the **reload factory-default dhcp-client-only-mode** command, the switch attempts to reach the DHCP server only the specified number of times.

If a DHCP server cannot be reached within the configured number of retries, the switch reverts to reloading in factory-default mode (see [Factory-Default Mode \(Mode A\)](#)); for example:

```
Unable to obtain a lease on first try. Exiting. interval 16ry
  Sending DHCP request
Unable to obtain a lease on first try. Exiting. interval 35ry
  Sending DHCP request
Retry count (of 3) expired! DHCP offer not received. interval 12ry
Switching from dhcp-client-only to factory-default!
```


Bare Metal Provisioning CLI 1.5

Overview

Bare Metal Provisioning CLI 1.5 is supported on the [S55](#) [S60](#) platforms.

- Bare Metal Provisioning version 3.0 is supported on the S4810, S4820T, and Z9000 switches.

In a data center network, Bare Metal Provisioning (BMP) automates the configuration and updating of switches, ensuring standard configurations across installed devices.

You can configure auto-configuration on a single switch or on multiple switches. BMP allows you to set up a stack with a minimum of effort, but is also useful for quick configuration of a single switch.

BMP eases configuration in the following key areas:

- On S55 and S60 switches running BMP 1.5:
 - An IP address, a running configuration and boot image are obtained from a DHCP server.
 - Switch access is allowed through a management port with or without DHCP-based dynamic IP address configuration of a switch. (BMP 1.5 supports access to a switch only on management ports, not on user ports.)
 - A switch boots up in Layer 2 mode with interfaces already in **no shutdown** mode and some basic protocols enabled to protect the switch and the network.

Commands

- [reload factory-default](#)
- [reload factory-default dhcp-client-mode](#)
- [reload factory-default dhcp-client-only-mode](#)
- [reload factory-default dhcp-server-mode](#)
- [stop jump-start](#)

reload factory-default

S55 S60

BMP 1.5 auto-configuration mode A: Reload the switch with the FTOS image stored in the local flash and apply the factory-default startup configuration. A temporary management IP address (192.168.0.1) is created.

Syntax

reload factory-default

Defaults

Loads the factory-default startup configuration file (see Example below).

Command Modes

EXEC Privilege

Command History

Version 8.3.5.0 Introduced on the S55.

Version 8.3.3.1 Introduced on the S60.

Usage Information

This is the reload mode when a new Dell Networking switch (without BMP) arrives. You can replace the temporary management IP address with a user-configured management IP address. The IP address 192.168.0.1 continues to be active for ten minutes. After ten minutes, a user-configured IP address is applied to the management interface.

Example

The factory-default startup configuration file is as follows:

```
interface range GigabitEthernet 0/0 - 47
  no shutdown
  switchport
  !
interface range TenGigabitEthernet 0/48 - 51
  no shutdown
  switchport
  !
interface ManagementEthernet 0/0
  ip address 192.168.0.1/24
  no shutdown
  !
ip telnet server enable
!
ip ssh server enable
!
protocol spanning-tree rstp
  no disable
!
protocol lldp
  no disable
  advertise dot1-tlv port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-description system-name
  advertise med
no disable
!
```

reload factory-default dhcp-client-mode

S55 S60

BMP 1.5 auto-configuration mode C: Reload a switch in DHCP-client mode with a specified FTOS image and a startup configuration file.

Syntax `reload factory-default dhcp-client-mode [honor-startup-config]`

| | | |
|-------------------|-----------------------------|---|
| Parameters | honor-startup-config | Honor the startup configuration file stored in the local flash. If this option is not entered, retrieve the configuration file from the configured file server. |
|-------------------|-----------------------------|---|

Defaults This is the default reload mode when a new Dell Networking switch configured with BMP arrives. The switch contacts a DHCP server to download an FTOS image and configuration file. If no DHCP server responds, the system reloads in factory-default mode.

Command Modes EXEC Privilege

| | | |
|------------------------|-----------------|------------------------|
| Command History | Version 8.3.5.0 | Introduced on the S55. |
| | Version 8.3.3.1 | Introduced on the S60. |

reload factory-default dhcp-client-only-mode

S55 S60

BMP 1.5 auto-configuration mode D: Reload the switch in DHCP-client-only mode with a specified FTOS image and startup configuration file for a specified number of discovery attempts.

Syntax `reload factory-default dhcp-client-only-mode [retries] [honor-startup-config]`

| | | |
|-------------------|-----------------------------|---|
| Parameters | <i>retries</i> | Enter the number of times that the switch attempts to reach a DHCP server. If no number of retries is entered, the switch continues to try to locate a DHCP server an infinite number of times and does not complete reloading. Range: 2 - 214748364 Default: Infinite number of retry attempts. |
| | <i>honor-startup-config</i> | Honor the startup configuration file stored in the local flash. If this option is not entered, retrieve the configuration file from the configured file server. |

Defaults The switch reloads by attempting to contact a DHCP server to download the FTOS image and startup configuration file. By default, an infinite number of retries are attempted.

When a switch that is reloading in DHCP-client-only mode cannot reach a DHCP server and has a number of retries configured, the switch attempts to reach the DHCP server only the specified number of times. If a DHCP server cannot be reached within the configured number of retries, the switch reloads in factory-default mode.

Command Modes EXEC Privilege

Command History

| | |
|-----------------|------------------------|
| Version 8.3.5.0 | Introduced on the S55. |
| Version 8.3.3.1 | Introduced on the S60. |

Usage Information

Important: Do not use Mode D unless the DHCP, DNS, and file servers are already configured. If the servers are not configured in the network, a switch endlessly attempts to discover the DHCP and other servers and does not complete the reload.

reload factory-default dhcp-server-mode

S55 S60

BMP 1.5 auto-configuration mode B: Reload the switch using the FTOS image stored in the local flash and apply the factory-default and DHCP server configurations. The switch boots up with a temporary management IP address (192.168.0.1/24) and functions as a DHCP server.

Syntax reload factory-default dhcp-server-mode

Defaults None

Command Modes EXEC Privilege

Command History

Version 8.3.5.0 Introduced on the S55.

Version 8.3.3.1 Introduced on the S60.

Usage Information

You must replace the temporary management IP address within ten minutes with a user-configured, permanent management IP address in order to secure the switch. During the first ten minutes, after authentication is enabled, access to the switch does not require a password.

stop jump-start

S55 S60

Z S4810

BMP 2.0: Stop the switch from reloading in Jumpstart mode to prevent a loop from occurring.

Syntax

stop jump-start

Note: This command has been deprecated on the S4810 and Z9000 platforms. It is replaced by the **stop bmp** command on those platforms.

Defaults

None

Command Modes

EXEC Privilege

Command History

| | |
|------------------|---|
| Version 9.1(0.0) | Deprecated command on the S4810 and Z9000 platforms. Replaced by the stop bmp command. |
| Version 8.3.11.4 | Introduced on the Z9000. |
| Version 8.3.10.1 | Introduced on the S4810. |
| Version 8.3.5.0 | Introduced on the S55. |
| Version 8.3.3.1 | Introduced on the S60. |

Usage Information

Use the **stop jump-start** command on a switch running BMP 2.0 if the switch enters a loop while reloading in Jumpstart mode because it is continuously trying to contact a DHCP server and a DHCP server is not found. The **stop jump-start** command stops the switch from connecting to the DHCP server. The startup configuration file stored in the local flash on the switch is loaded as part of the **stop jump-start** command.

Bare Metal Provisioning 3.0

Bare metal provisioning 3.0 (BMP 3.0) is included as part of the Dell Networking operating system (FTOS) image. BMP 3.0 is supported on the **S4810** **S4820T** **Z**, and MXL Switch platforms.

Overview

BMP improves operational efficiency to the system by automatically loading pre-defined configurations and FTOS images using standard protocols such as dynamic host configuration protocol (DHCP) and common file transfer mechanisms.

Bare metal provisioning:

- reduces the time to install and configure the network device.
- helps eliminate configuration errors and ensure consistent configurations.
- functions on a single system or on multiple systems.
- includes SNMP support.
- includes support for pre- and post configuration scripts.

With BMP 3.0, the system can retrieve a configuration file or a preconfiguration script indicated in the DHCP offer. Using the preconfiguration script, you can:

- verify the integrity of the boot image downloaded from the DHCP offer.
- decide what type of configurations you want to apply based on factors such as your network reachability, port status, and neighbor discovery.
- monitor your CPU and memory utilization, your port traffic status, or perform link and topology checking with link layer discovery protocol (LLDP).
- retrieve a configuration from a central repository.

To execute CLI commands during boot time, the system uses an application called f10do.

If BMP is disabled and an auto-configuration script is available, the auto-configuration script is run. Once the script has completed, the startup configuration is applied.

Prerequisites

Before you use BMP 3.0 to auto-configure a supported Dell Networking switch, first configure the following.

- External dynamic host configuration protocol (DHCP) server (required) — a network device offering configuration parameters.
- File server (required) — a network device for storing and servicing files.
- Domain name server (DNS) (optional) — a server that associates domain names in the network with IP addresses.
- Relay agent (optional) — an intermediary network device that passes messages between DHCP clients and the DHCP server when the server is not on the same subnet. It can also provide IP addresses for multiple subnets.

For more information, refer to [Domain Name Server](#) and [File Server](#).

Important Information

BMP 3.0 is supported on the user ports and management ports of a switch.

If your network has VLT enabled on aggregator switches and you are configuring the ToR switch to load using BMP, configure the aggregator switches with the **lacp ungroup member-independent vlt** command if the DHCP and file servers are reachable via the interface configured as part of VLT LAG.

BMP eases configuration in the following ways:

- Switch access is allowed through all ports (management and user ports) with or without DHCP-based dynamic IP address configuration of a switch.
- Booting up in Layer 3 mode with interfaces already in No Shutdown mode and some basic protocols enabled to protect the system and the network.
- To access the configuration file or a preconfiguration script, use the DHCP offer.
- Download and execute scripts before configurations are applied allowing preconfiguration checks on the switch.

Standard Upgrades with BMP

Standard upgrades performed with BMP enabled provide a fallback mechanism allowing switches to be returned to their previous state.

Switches normally have two partitions to store images. You can select which partition the switch uses to boot up. BMP always downloads and saves the image in the inactive partition. When BMP reloads, it automatically activates this partition so the switch boots up with the newly downloaded image.

The downloaded configuration is copied to the running configuration and then applied to the switch.



Note: The downloaded configuration does not override the startup configuration.

Verify the operation and performance of the new image and the configuration on the switch before committing the changes. After the changes are deemed correct, commit them by performing the following steps in the order given:

1. Disable BMP with the **reload-type normal-reload** command.
2. Make the activating partition permanent with the **boot system** command.
3. If you did not enable auto-save, manually override the startup configuration file using the write memory command.



Note: If you did not enable auto-save, the switch automatically overrides the startup configuration.

You can revert to the previous state by not committing the changes, disabling BMP, activating the previous partition and reloading the switch.

BMP Process Overview

When the system boots up in default BMP mode, the following items are requested.

1. Current (new) FTOS build image.
2. Configuration file or preconfiguration script (EXPECT, TCL, or Z-shell [ZSH] script).
3. A list of checksums for all these components.



Note: The configuration file maintains normal BMP functionality when a preconfiguration script is not sent.

Preparing BMP

The following sections describe how to prepare BMP:

- [DHCP Server](#)
- [File Server](#)
- [Domain Name Server](#)

DHCP Server

To configure the DHCP server use the following information.

DHCP Configuration

Before you can use BMP mode on a switch, first configure a DHCP server.

Configure the DHCP server with the following set of parameters for each client switch. For more information, refer to the *FTOS Configuration Guide, Dynamic Host Configuration Protocol* chapter. To assign an IP to the system and other parameters, configure the DHCP server.

Update the following parameters on the appropriate DHCP server:

- **Boot File Name** — the FTOS image loaded on the system. Option 67 in the DHCP offer is the boot file name; the filename is BOOTP payload. If both are specified, option 67 is used. The system supports the TFTP, HTTP, HTTPS, SFTP, SCP, FTP, FLASH and USBFLASH protocols.
- **Configuration File Name** — the configurations applied to the system. The configuration file name is expected to use option 209. A preconfiguration script can also be given in option 209 to configure the device by itself for a download configuration file.
- **File Server Address** — the server where the Image and Configurations files are placed. The address is assumed to be a TFTP address unless it is given as a URL. The system supports the TFTP, HTTP, HTTPS, SFTP, SCP, and FTP protocols, as well as files stored in Flash.
- **Domain Name Server (Optional)** — the DNS server contacted to resolve the host name.
- **IP Address** — dynamic IP address for the system. Use this IP address only for file transfers.

The following lists the DHCP option codes.

| | |
|-----|-------------------------|
| 6 | Domain Name Server IP |
| 60 | Vendor class identifier |
| 61 | Class identifier |
| 66 | TFTP Server name |
| 67 | Boot filename |
| 150 | TFTP server IP address |
| 209 | Configuration file |
| 230 | User port stacking |



Note: BMP eventually exits when a timeout occurs.

In the following scenarios, BMP requests a different DHCP offer.

- If you enable the **reload-type config-scr-download enable** command, the DHCP offer specifies both the boot image and the configuration file. If either download is successful, BMP does not request another DHCP offer.
- If the offer contains only a boot image that cannot be downloaded, BMP requests another DHCP offer.
- If you enable the **reload-type config-scr-download enable** command and the configuration file in the offer cannot be downloaded, BMP requests another DHCP offer.

DHCP Server IP Blacklist

If the process does not complete successfully, the DHCP server IP is blacklisted and the BMP process is re-initiated.

A DHCP server IP is maintained in the blacklist for 10 minutes. If a DHCP offer is received from the blacklisted DHCP server, the offer is rejected until the IP is alive in the blacklist (10 minutes).

MAC-Based Configuration

One way to use the BMP mode most efficiently is to configure the DHCP server to assign a fixed IP address, FTOS image, and configuration file based on the system's MAC address.

When this configuration is done, the same IP address is assigned to the system even on repetitive reloads and the same configuration file is retrieved when using the DNS server or the network-config file to determine the hostname.

The assigned IP address is only used to retrieve the files from the file server. It is discarded after the files are retrieved.

Following is an example of a configuration of the DHCP server included on the most popular Linux distribution. The `dhcpd.conf` file shows the MAC-based IP and configuration file assignment are fixed.

Table 5-1. MAC-Based Configuration

| Parameter Example | |
|--|---|
| <pre>option configfile code 209=text; option bootfile-name code 67=text; host HOST1{</pre> | |
| #####MAC to IP mapping | |
| <pre>hardware ethernet 00:01:e8:8c:4d:0e; fixed-address 30.0.0.20;</pre> | |
| #####Config file name could be given in the following way | FTP URL with IP address HTTP URL with DNS TFTP |
| <pre>option configfile "ftp://admin:admin@30.0.0.1/ pt-s4810-12"; option configfile "http://Guest-1/pt-s4810-12"; option configfile "pt-s4810-12";</pre> | |
| #####bootfile-name could be given in the following way | FTP URL with DNS HTTP URL with IP address TFTP URL with IP address |
| <pre>option bootfile-name "ftp:// admin:admin@Guest-1/FTOS-SE-8.3.10.1.bin"; option bootfile-name "http://30.0.0.1/ FTOS-SE-8.3.10.1.bin";</pre> | |

File Server

Set up a file server and ensure connectivity.

To allow file transfers to the switch, configure the file server that holds the boot and configuration files. The system recognizes HTTP, TFTP, FTP, USB, and Flash URLs.

For example:

- tftp://server ip or name/filename
- ftp://user:passwd@serverip or name//mypath/FTOS-A.B.C.D.bin
- flash://filename
- http://server ip
- name/filename

When loading the FTOS image, if the FTOS image on the server is different from the image on the local Flash, the system downloads the image from the server onto the local Flash and reloads using that image. If the FTOS image on the server is the same image, the system loads the configuration file, if present, or the startup-config without downloading a new image.

Domain Name Server

To determine the host name applied in the switch startup configuration, when no configuration file is retrieved from the DHCP server, set up a domain name server (DNS).

The DNS server is contacted only when no configuration file is contained in a DHCP server response and the host name is not resolved from the network-config file on the switch. For more information, refer to the *FTOS Configuration Guide, IPv4 Addressing* chapter, *Resolution of Host Names* section.

Reload Modes

BMP supports two types of reload modes: BMP mode and Normal mode.

This section describes the following Reload modes.

- [BMP Mode](#)
- [Normal Mode](#)
- [DHCP Configuration](#)
- [FTOS Image Retrieval](#)

BMP mode is the default boot mode configured for a new system arriving from Dell Networking. This mode obtains the FTOS image and configuration file from a network source (DHCP and file servers).

To boot the switch up with the management port in No Shutdown mode, use Normal mode. If the management IP address is present in the start-up configuration file, it is assigned. If the management IP address is not present in the start-up configuration file, no IP address is assigned to the management interface.

BMP Mode

The following sections describe BMP mode:

- [BMP Mode Prerequisites](#)
- [MAC-Based IP Address Assignment](#)

BMP Mode Prerequisites

To auto-configure a switch, before you use BMP mode, first configure a DHCP, DNS, and file server in the network.

On a new factory-loaded switch, the switch boots up in default BMP mode to facilitate configuration of the switch. You can reconfigure a switch to reload between BMP and Normal mode.

- BMP mode (default) — the switch automatically configures all ports (management and user ports) as Layer 3 physical ports and acts as a DHCP client on the ports for a user-configured time (DHCP timeout). Set BMP mode using the **reload-type bmp** command.

- Normal mode — the switch loads the FTOS image and startup configuration file stored in the local Flash. New configurations require that you manually configure the Management IP and Management Interface. Set Normal mode using the **reload-type normal-reload** command.



Note: To apply the startup configuration, cancel the default BMP setup using the **stop bmp** command from the console. To disable BMP for the next reload, use the **reload-type normal-reload** command.

MAC-Based IP Address Assignment

To assign a fixed IP address and configuration file based on the system's MAC address, one way to deploy BMP mode is to configure the DHCP server. In this way, the same IP address is assigned and the same configuration file is retrieved when the switch reloads.

Using a dynamic IP address assignment may create a situation in which the desired configuration is not loaded on the system because the IP address changes each time the system is reloaded.

For example, on a DHCP3 server, you can configure the assignment of a fixed MAC-based IP address and configuration file by entering the following lines of configuration parameters in the *dhcpd.conf* file on the server:

```
host S4810 {
    hardware ethernet 00:01:e8:81:e2:39;fixed-address
    20.0.0.48;option configfile "customer.conf";
}
```

Normal Mode

When reloaded in Normal mode, the switch boots up with the management port in No Shutdown mode.

If the management IP address is present in the start-up configuration file, it is assigned. If the management IP address is not present in the start-up configuration file, no IP address is assigned to the management interface. You can connect to the management port with an IP address on the same network and log in to the system through a telnet or SSH session.

To configure a switch to reload using Normal mode, use the following step:

- The switch reloads in Normal mode using the FTOS image and startup configuration file stored in the local Flash.

GLOBAL CONFIGURATION mode

```
reload-type normal-reload
```

DHCP Configuration

Normal mode does not require a separate DHCP server configuration.

FTOS Image Retrieval

The FTOS image is loaded from the local Flash.

Scripts

With FTOS version 9.1(0.0), the system supports a scripting environment when a BMP or Normal reload occurs. BMP uses pre- and post configuration scripts, while a Normal reload uses an auto-execution script.

Preconfiguration Scripts

Previously, FTOS accessed the configuration file or image file from the DHCP server.

With BMP 3.0, FTOS accesses the image, then the configuration file or preconfiguration script from the DHCP offer. Use preconfiguration scripts to:

- verify the integrity of the FTOS image downloaded from the DHCP offer.
- dynamically decide what types of configurations to apply to your system based on various factors such as network reachability, port status, neighbor discovery.
- use LLDP to monitor and generate reports periodically for CPU and memory utilization, port traffic status, and perform link and topology checking.

You can provide a preconfiguration script in DHCP option 209 to either configure the switch or download a configuration file. The script can download a configuration file or apply CLI commands. In the downloaded configuration, post configuration script CLIs are executed if present.

Schedule preconfiguration scripts to run on selected dates and at a specified time, or when CPU or memory usage is low to avoid system impacts. You can set the system to retry downloading a configuration up to six times or to automatically save the downloaded configuration or script on the switch.

After the configuration is applied, it can trigger a post configuration script to ensure the configurations and switch functions are correct. This post configuration script can only be triggered when the preconfiguration script is run.

Define configuration parameters on the DHCP server for each chassis based on the chassis MAC address.

The system supports preconfiguration scripts in EXPECT, TCLSH, and ZSH.



Note: Dell Networking recommends adding the following f10do wrapper function at the beginning of TCLSH and EXPECT scripts to display a properly formatted output string:

```
# Execute F10do and return the output string
proc ExecF10Do {cmd_str} {
  set str [exec f10do "$cmd_str"]
  set tmp_str [string map {\n \r\n} $str ]
  return $tmp_str
}
...
set out_str [ExecF10Do "show version"]
puts $out_str
...
```

Post Configuration Scripts

In BMP 3.0, after the preconfiguration script completes and the configuration loads, you can run a post configuration script if one is present in the configuration file.

To check the status of configured ports or protocols which can then be sent as a status report to a central repository for your network administrators, use the post configuration script. To set the host name of the system or perform additional configuration settings, use the post configuration script. The system supports post configuration scripts in EXPECT, TCLSH, and ZSH. If you installed SmartScripts in FTOS, the system also supports post configuration scripts in PERL and Python.

Auto-Execution Scripts

The function of an auto-execution (auto-exec) script is the same as a preconfiguration script except that it is executed on every reboot in Normal mode.

Store scripts in a `flash://autoexec` file. Auto-exec scripts are independent of BMP.

The auto-exec script only executes when:

- BMP is disabled.
- the script is stored in a `flash://autoexec` file.
- when you use the `reload-type normal-reload` command before you reload the system.

If the auto-exec script fails, the system generates a message indicating the failure and does not load the configuration file. Before continuing the upgrade, correct the error in the script.

Preconfiguration Process for Scripts

To preconfigure scripts, follow these steps:

1. Decide what information you want to preconfigure; for example, request username and password information. Verify the integrity of the boot image downloaded from the DHCP offer and apply configuration types.
2. Create a preconfiguration script in EXPECT, TCL or ZSH. The script cannot be binary.
3. Store the script on the DHCP server in the DHCP offer.
4. Apply the FTOS upgrade. The system boots in BMP default mode and runs the preconfiguration script.
 - The default timer on the script is 10 minutes. The maximum amount of time the script can run is 1 hour.
5. The system receives an IP address via the DHCP server which it uses to get an FTOS image to boot, a configuration file (if supplied), and a preconfiguration script.
 - During the preconfiguration process, a connection to a dedicated instance of the CLI is available.
6. The preconfiguration script can access FTOS CLI commands through the support of the **f10do** application. The **f10do** application has no pagination, is always set to “terminal length 0”, and has FTOS CLI privilege 15 enabled. It works in the following modes:
 - Continuous mode (**f10do** command) — use to retain the FTOS context.
 - Reset mode (**f10do-r** command) — use to reset the CLI command to its original context.

Configuration Tasks

When the system boots up in BMP mode, all ports, including management ports, are placed in L3 mode in a No Shut state.

The system acts as a DHCP client on these ports for a time (dhcp-timeout). This state allows the system time to send out a DHCP DISCOVER on all the interface up ports to the DHCP server in order to obtain its IP address, boot image filename, and configuration file or preconfiguration script from the DHCP server.

- Set up a DHCP server. For more information, refer to the *Dynamic Host Configuration Protocol* chapter in the *FTOS Configuration Guide*. Configure the DHCP server to assign an IP address to each system along with the following DHCP server parameters:
 - IP address pool — IP address for the system.
 - Image name — FTOS image used to boot up the system.

- Configuration file — Start up configuration parameters or preconfiguration script to be applied to the system.
- IP address of TFTP file server — File server from which the image and startup configuration file or preconfiguration script are downloaded.
- Domain name server — DNS server to be contacted to resolve the host name.

Use the following DHCP option codes in the *dhcpd.conf* file.

- 6 — IP address of the domain name server, if you need a DNS server to resolve the IP address of a file server host name.
- 150 — IP address of a TFTP server.
- 209 — configuration file or preconfiguration script.
- 230 — user port stacking.

For example, a sample *dhcpd.conf* file on a DHCP3 server is as follows:

```
lease-file-name "/var/lib/dhcpd/dhcpd.leases";
option configfile code 209 = text;
option tftp-server-address code 150 = ip-address;
subnet 20.0.0.0 netmask 255.255.255.0 {
    range 20.0.0.26 20.0.0.28;
    filename "FTOS-SC-1-2-0-363.bin";
    option configfile "customer.conf";
    option tftp-server-address 20.0.0.1;
    option domain-name-servers 20.0.0.1;
    option #230 "unit-number:3#priority:2#stack-group:0"
}
```

- Set up a TFTP server and ensure connectivity.

Configure a TFTP file server as the network source from which the switch downloads the image file and the configuration file or preconfiguration script to be applied to the system. On a TFTP server, the required files are commonly stored in the */tftpboot* directory.

When the switch is loaded in BMP mode, if the FTOS image on the file server (image path given by DHCP server) is different from the image stored in local Flash memory, the system downloads the image on the file server into the local Flash and reboots using that image. If the image is the same, no action is performed. The switch tries to download the configuration file.

- Set up a DNS server. For more information, refer to the *IPv4 Addressing* chapter in the *FTOS Configuration Guide, Resolution of Host Names* section.

If the DHCP server response does not specify a configuration file or preconfiguration script and the host name is not resolved using the network-config file, configure the DNS server to determine a system's host name and the correct configuration file or preconfiguration script to be downloaded on the system.

If no configuration file or preconfiguration script is present in the DHCP offer, the startup configuration is applied after the BMP exit is complete. The system does not fall back to the network-config file or the system host name file.

System Boot and Set-Up Behavior in BMP Mode

The following steps describe the system boot up process:

1. The system begins the boot up process in BMP mode (the default mode).
2. The system sends DHCP discover on all the interface up ports.

```
00:01:31: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Ma 0/0.
00:01:31:%STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Te 0/0.
00:01:31: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Te 0/5.
00:01:31: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Te 0/6.
00:01:47: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Te 0/8.
00:01:47: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVERsent on Te 0/35.
00:01:47: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Fo 0/56.
00:01:47: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Fo 0/60.
00:01:47: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Ma 0/0.
```
3. The IP address, boot image filename, and configuration filename are reserved for the system and provided in the DHCP reply (one-file read method). The system receives its IP address, subnet mask, DHCP server IP, TFTP server address, DNS server IP, bootfile name, and configuration filename from the DHCP server.

If a DHCP offer has neither an image path or configuration file path, it is considered an invalid BMP DHCP offer and the offer is ignored. The first DHCP offer with IP address, FTOS image and configuration file or preconfiguration script, or the IP address and FTOS image, or the IP address and configuration file or preconfiguration script is chosen.

4. The DHCP OFFER is selected.

All other ports except the port on which the offer was received and selected are set to Shutdown mode.

- ```
00:01:33: %STKUNIT0-M:CP %JUMPSTART-5-DHCP_OFFER: DHCP acquired
I P 30.0.0.20 mask 255.255.0.0
server IP 30.1.1.1.
00:01:33: %STKUNIT0-M:CP %JUMPSTART-5-DHCP_OFFER: DHCP tftp I P
30.0.0.1 dns I P 30.0.0.1 router
IP 30.0.0.14.
00:01:33: %STKUNIT0-M:CP %JUMPSTART-5-DHCP_OFFER: DHCP image
file FTOS-SE-8.3.10.1.bin.
00:01:33: %STKUNIT0-M:CP %JUMPSTART-5-DHCP_OFFER: DHCP config
file pt-s4810-12.
00:01:33: %STKUNIT0-M:CP %JUMPSTART-5-DHCP_OFFER: DHCP stacking
info NIL.
```
5. The system sends a message to the server to retrieve the named configuration file or preconfiguration script and/or boot file from the base directory of the server.

- a If you use the optional **bootfile-name** command, the filename can be 256 bytes. If a filename field is specified in the DHCP offer, the filename can be 128 bytes. The name can be a fully qualified URL or it can be a filename only.
- b When an FTOS build image is found, the system compares that build image to the version currently loaded on the chassis.
- If there is a mismatch between the build images, the system upgrades to the downloaded version and reloads.

```
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Major Version: 1
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Minor Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Main Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Patch Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Major
Version : 9
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Minor
Version : 1
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Main
Version : 0
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Patch
Version : 222
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-2-JUMPSTART_DOWNLOAD_START: The FTOS image download
has started.Erasing IOM Primary Image, please
wait.....
.....
```

- If the versions match, the system downloads the configuration file or preconfiguration script.

```
00:03:19: %STKUNIT0[]M: CP
%JUMPSTART[]5[]JUMPSTART_DWNLD_CONFIG_SCRIPT_SUCCESS: The
config/script file download is successful
00:03:19: %STKUNIT0[]M:CP
%JUMPSTART[]2[]JUMPSTART_DOWNLOAD_START: The config file
download has started.
00:03:19: %STKUNIT0[]M:CP %JUMPSTART[]5[]JUMPSTART_DOWNLOAD:
The config file download is successful.
00:03:19: %STKUNIT0-M:CP %JUMPSTART-5-CFG_APPLY: The downloaded
config from dhcp server is being applied
```

- c If you download the configuration file or preconfiguration script from the server, any saved startup configuration on the Flash is ignored. If you do not download the configuration file or preconfiguration script from the server, the startup configuration file on the Flash is loaded as in Normal reload.
6. When the FTOS build image and configuration file or preconfiguration script are downloaded, the IP address is released.

```
00:04:06: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART: DHCP RELEASE
sent on Fo 0/56.
00:04:06: %STKUNIT0-M:CP %IFMGR-5-ASTATE_DN: Changed interface
Admin state to down: Fo 0/56
```

7. The system applies the configuration. The system is now up and running and is managed as usual.

## BMP Mode: Boot and Set-UP Behavior

when a switch that is configured to reload in BMP mode boots up, one of the following scenarios may occur.

- [Reload Without a DHCP Server Offer](#)
- [Reload with a DHCP Server Offer Without an FTOS Offer](#)
- [Reload with a DHCP Server Offer and no Configuration File](#)
- [Reload with a DHCP Server Offer Without a DNS Server](#)
- [Preconfiguration Scripts](#)
- [Post Configuration Scripts](#)
- [Auto-Execution Scripts](#)

### Reload Without a DHCP Server Offer

A switch configured to reload in BMP mode. If the DHCP server cannot be reached, the system keeps on sending DISCOVER messages.

```
00:01:44: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Te 0/50.
00:01:44: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Te 0/51.
00:01:44: %STKUNIT0-M:CP %JUMPSTART-5-JUMPSTART_DISCOVER: DHCP
DISCOVER sent on Ma 0/0.
```

### Reload with a DHCP Server Offer Without an FTOS Offer

Switches configured to reload in BMP mode that reach a DHCP server but do not locate a downloadable FTOS image file on the server will attempt to download the configuration file.

1. The system boots up with the BMP application.

```
13:23:47: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP acquired
IP 10.16.134.167 mask 255.255.0.0 server
IP 10.16.134.207.
13:23:48: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP tftp IP
NIL sname NIL dns IP NIL router IP NIL.
13:23:48: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP image
file NIL.
13:23:48: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP config
file tftp://10.16.127.53/customer.conf.
13:23:49: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: stacking info
NIL.
```

2. The system downloads the customer.conf configuration file from the file-server address if you enabled config-scr-download.

- If the configuration download is successful, the following logs display.

```
R00:03:19: %STKUNIT0]M: CP
%JUMPSTART]5]JUMPSTART_DWNLD_CONFIG_SCRIPT_SUCCESS: The
config/script file download is successful
00:03:19: %STKUNIT0]M:CP
%JUMPSTART]2]JUMPSTART_DOWNLOAD_START: The config file
download has started.
00:03:19: %STKUNIT0]M:CP %JUMPSTART]5]JUMPSTART_DOWNLOAD:
The config file download is successful.
00:03:19: %STKUNIT0-M:CP %JUMPSTART-5-CFG_APPLY: The downloaded
config from dhcp server is being applied
00:03:24: %STKUNIT11]M:CP %SYS]5]CONFIG_LOAD: Loading
configuration file
```

## Reload with a DHCP Server Offer and no Configuration File

If a switch that is configured to reload in BMP mode reaches a DHCP server but cannot retrieve a configuration file, the switch looks for a configuration file on the file server only if you enabled `config-scr-download`.

- The system boots up with the BMP application.
- The system receives a DHCP offer from a DHCP server with the following parameters.

```
13:23:47: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP acquired
IP 10.16.134.167 mask 255.255.0.0 server
IP 10.16.134.207.
13:23:48: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP tftp IP
NIL sname NIL dns IP NIL router IP NIL.
13:23:48: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP image
file tftp://10.16.127.53/mxl.bin.
13:23:48: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: DHCP config
file NIL.
13:23:49: %STKUNIT0-M:CP %JUMPSTART-5-BOOT_OFFER: stacking info
NIL.
```

- The system downloads the build image from the file server.
- The system compares the current local build image to the downloaded build image as follows.
  - If the build image versions match, the system does not try to load any image and comes up with the FTOS prompt.

```
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Major Version: 1
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Minor Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Main Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Patch Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Major
Version : 100
:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Minor
Version : 0
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Main
Version : 0
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Patch
Version : 0
```

- b If the build images versions are different, the system stores the downloaded build image in the local Flash and loads the build image from the Flash. This process is repeated until the build image versions match.

```
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Major Version: 1
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Minor Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Main Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Downloaded Image
Patch Version :0
00:03:06: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Major
Version : 9
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Minor
Version : 1
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Main
Version : 0
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_RELEASE_HEADER_INFO: Flash A Image Patch
Version : 222
00:03:07: %STKUNIT0-M:CP
%JUMPSTART-2-JUMPSTART_DOWNLOAD_START: The FTOS image download
has started.Erasing Sseries Primary Image, please
wait.....
```

The system looks for the configuration file on the file server. If the system does not find a configuration file, the download fails. If the build image processing is successful, BMP stops. If the build image download also fails, the current offer is treated as invalid and BMP tries to send DISCOVER messages.

## Reload with a DHCP Server Offer Without a DNS Server

Reload FTOS on a switch using a preconfiguration script.

To reload FTOS on a switch using a preconfiguration script, the following must be true.

- BMP must be enabled.
- The download of the script is from an external server. The location is specified in the DHCP offer.
- The first line of the script must contain one of the following:
 

```
#!/usr/bin/expect
#!/usr/bin/tclsh
#!/usr/bin/zsh
```
- After the first line, but before the start of the script, the script must contain the signature `#/DELL-NETWORKING`.

**Note:** The `#/DELL-Force10` signature is also supported.

- The preconfiguration script is downloaded instead of the configuration file.
- The preconfiguration script is run before applying the start-up configuration file.

- The preconfiguration script has the ability to use configuration FTOS CLI commands using the `f10do` application.
- When the preconfiguration script completes, the start up configuration file is automatically applied.

If a preconfiguration script file download is successful, the following SYSLOGs display.

```
00:01:52: %STKUNIT11-M:CP
%JUMPSTART-2-JUMPSTART_DOWNLOAD_START: The config file download
has started.
00:01:53: %STKUNIT11-M:CP
%JUMPSTART-5-JUMPSTART_DWNLD_CONFIG_SCRIPT_SUCCESS: The
config/script filedownload is successful.
00:01:54: %STKUNIT11-M:CP
%JUMPSTART-5-JUMPSTART_DWNLD_FILE_IS_SCRIPT_FILE: The
downloaded file is a script file.
00:01:54: %STKUNIT11-M:CP
%JUMPSTART-5-JUMPSTART_PRE_CONFIG_SCRIPT_BEGIN: The Pre-Config
Script has started to Execute.
```

After the preconfiguration script successfully executes, the startup configuration file loads.

```
00:02:00: %STKUNIT11-M:CP
%JUMPSTART-5-JUMPSTART_PRE_CONFIG_SCRIPT_END: Pre-Config
script executed successfully.
00:02:01: %STKUNIT11-M:CP %SYS-5-CONFIG_LOAD: Loading
configuration file
```

If a post configuration script is present in the applied configuration file, it executes and the following logs display:

```
00:03:11: %STKUNIT0-M:CP %SYS-5-CONFIG_LOAD: Loading
configuration file
00:03:11: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/48
00:03:11: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/49
00:03:11: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/50
00:03:11: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/51
00:03:12: %STKUNIT0-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Ma 0/0
00:03:12: %STKUNIT0-M:CP
%JUMPSTART-5-JUMPSTART_POST_CONFIG_SCRIPT_BEGIN: The
Post-Config Script has started to Execute Fri Dec 7 01:38:04
GMT 2012
00:03:13: %STKUNIT11-M:CP
%JUMPSTART-5-JUMPSTART_POST_CONFIG_SCRIPT_END: Post-Config
script executed successfully.
```

If a post configuration script is not present in the applied configuration file, the following logs display:

```
00:02:01: %STKUNIT11-M:CP %SYS-5-CONFIG_LOAD: Loading
configuration file
00:02:04: %STKUNIT11-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Ma 0/0
00:02:04: %STKUNIT11-M:CP
%JUMPSTART-5-JUMPSTART_POST_SCRIPT_NOT_PRESENT: The
Post-Config Script is not present.
```



## Using the Post Configuration Script (BMP Mode Only)

To reload FTOS on a switch using a preconfiguration script, the following conditions must be true:

- BMP must be enabled.
- You can write the post configuration script in EXPECT, TCLSH, or ZSH. If you already installed the SmartScripts package, you can also write the post configuration script in PERL or Python.
- No restraints are required for the post configuration script, such as the signature `#/DELL-NETWORKING` that is required for the preconfiguration script.

**Note:** The `#/DELL-Force10` signature is also supported.

- Configure the post configuration script by using the **script post-config** command.
- The post configuration script must be executed after the start-up configuration process required by BMP has been applied.
- The post configuration script has the ability to use configuration FTOS CLI commands using the application name `F10do`.

## Reload Using the Auto-Execution Script (Normal Mode Only)

To use the auto-execution script, the following conditions must be true:

- BMP must be disabled.
- Always store the auto-execution script in `flash://autoexec`.
- You can write the auto-execution script in EXPECT, TCLSH, or ZSH. If you already installed the SmartScripts package, you can also write the post configuration script in PERL or Python.
- No restraints are required for the auto-execution script, such as the signature `#/DELL-NETWORKING` that is required for the preconfiguration script.

**Note:** The `#/DELL-Force10` signature is also supported.

- The auto-execution script has the ability to use configuration FTOS CLI commands using the application name `F10do`.
- When the auto-execution script is complete, the start-up configuration is applied depending on the return status of the script:
  - Success – 0 — the start-up configuration is applied.
  - Failure — non-zero — the start-up configuration is not applied.

If the system is rebooted with `reload-type` set as `normal-reload` and an auto-execution script is present in the Flash directory, the following logs display:

```
Starting Dell Force10 application
00:00:13: %STKUNIT1-M:CP %RAM-6-ELECTION_ROLE: Stack unit 1 is
transitioning to Management unit.
00:00:15: %STKUNIT1-M:CP %CHMGR-5-STACKUNITDETECTED: Stack unit
1 present
00:00:16: %STKUNIT1-M:CP %JUMPSTART-5-AUTOEXEC_START:
```

After the script execution is successful, FTOS displays the following log:

```
00:00:49: %STKUNIT1-M:CP %JUMPSTART-5-AUTOEXEC_SUCCESS:The
AutoExec Script execution returned Success.
00:00:51: %STKUNIT1-M:CP %SYS-5-CONFIG_LOAD: Loading
configuration file
```

If the script returns a non-zero value (indicating a failure), the configuration file does not load in the system. You must debug it manually and reload the system with corrected script. If the auto-exec script fails, the system displays the following syslog:

```
00:00:34: %STKUNIT1-M:CP %JUMPSTART-5-AUTOEXE_FAILURE: The
AutoExec Script execution returned Failure.
```

## Script Examples

The following are BMP script examples.

### Auto-Execution Script - Normal Mode

```
FTOS#show reload-type
Reload-Type : normal-reload [Next boot : normal-reload]
FTOS#show file flash://autoexec
#! /usr/bin/tclsh
puts [exec f10do "show version"]
puts [exec date]
puts "this is Autoexec script"
FTOS#
FTOS#
FTOS#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload [confirm yes/no]: yes
00:32:16: %STKUNIT1-M:CP %CHMGR-5-RELOAD: User request to
reload the chassis syncing disks... done
unmounting file systems...
unmounting /f10/flash (/dev/ld0h)...
unmounting /usr/pkg (/dev/ld0g)...
unmounting /usr (mfs:35)...
unmounting /f10 (mfs:21)...
unmounting /kern (kernfs)...
unmounting / (/dev/md0a)... done
rebooting
b..
..
..
Starting Dell Force10 application
00:00:13: %STKUNIT1-M:CP %RAM-6-ELECTION_ROLE: Stack unit 1 is
transitioning to Managementunit.
00:00:15: %STKUNIT1-M:CP %CHMGR-5-STACKUNITDETECTED: Stack unit
1 present
```

The following line indicates the start of the auto-execution script.

```
00:00:16: %STKUNIT1-M:CP %JUMPSTART-5-AUTOEXEC_START:
00:00:19: %STKUNIT1-M:CP %CHMGR-5-CHECKIN: Checkin from Stack
unit 1 (type S4810, 64 ports)
00:00:20: %00:00:20: %STKUNIT1-M:CP %CHMGR-0-PS_UP: Power
supply 0 in unit 1 is up
00:00:20: %STKUNIT1-M:CP %CHMGR-5-STACKUNITUP: Stack unit 1 is
up
00:00:21: %STKUNIT1-M:CP %CHMGR-5-SYSTEM_READY: System ready
00:00:21: %STKUNIT1-M:CP %RAM-5-STACK_STATE: Stack unit 1 is in
Active State.
00:00:22: %STKUNIT1-M:CP %IFMGR-5-OSTATE_UP: Changed interface
state to up: Ma 1/0
00:00:26: %S4810:1 %IFAGT-5-INSERT_OPTICS: Optics SFP inserted
in slot 1 port 30
00:00:27: %STKUNIT1-M:CP %CHMGR-5-PSU_FAN_UP: Fan 0 in PSU 0 of
Unit 1 is up
00:00:29: %S4810:1 %IFAGT-5-INSERT_OPTICS_PLUS: Optics SFP+
inserted in slot 1 port 11
00:00:36: %STKUNIT1-M:CP
%IFMGR-5-IFM_ISCSI_ACL_REGION_NOT_ALLOCATED: iSCSI Session
monitoring cannot be enabled without ACL regions allocated to
it. To enable iSCSI SessionMonitoring allocate cam-blocks to
iscsiopacl using cam-acl CLI and then save and reload.
00:00:36: %STKUNIT1-M:CP %IFMGR-5-IFM_ISCSI_ENABLE: iSCSI has
been enabled causing flowcontrol to be enabled on all
interfaces. EQL detection and enabling iscsi
profile-compellent on an interface may cause some automatic
configurations to occur like jumbo frames on allports and no
storm control and spanning tree port-fast on the port of
detection
00:00:36: %STKUNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful
on consoleFTOS>FTOS#terminal length 0
```

The following line indicates that the auto-execution script is executing:

```
FTOS#show version
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 2.0
Dell Force10 Application Software Version: 1-0(0-338)
Copyright (c) 1999-2012 by Dell Inc. All Rights Reserved.
Build Time: Thu Dec 27 21:32:28 2012
Build Path: /sites/sjc/work/build/buildSpaces/build06/
FIT-INDUS-1-0-0/SW/SRC
System image file is "dt-maa-s4810-72"
System Type: S4810Control
Processor: Freescale QorIQ P2020 with 2147483648 bytes of
memory.
128M bytes of boot flash memory.
1 52-port GE/TE/FG (SE)48 Ten GigabitEthernet/IEEE 802.3
interface(s)
4 Forty GigabitEthernet/IEEE 802.3 interface(s)
FTOS#Wed Jan 2 22:47:34 GMT 2013
this is Autoexec script
```

The following line indicates the auto-execution script has completed successfully:

```
00:00:49: %STKUNIT1-M:CP %JUMPSTART-5-AUTOEXEC_SUCCESS:
The AutoExec Script execution returned Success.
```

The following line indicates that the configuration file is loaded into the switch:

```

FTOS#00:00:51: %STKUNIT1-M:CP %SYS-5-CONFIG_LOAD:
Loading configuration file
00:00:52: %STKUNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/36
00:00:53: %STKUNIT1-M:CP %IFMGR-5-ASTATE_DN: Changed interface
Admin state to down: Ma 0/0
expect "ftp>"
send "cd scripts\n"
expect "ftp>"
send "ls\n"
expect "ftp>"
send "get $post_conf\n"
expect "ftp>"
send "get $config_file\n"
expect "ftp>"
send "bye\n"
expect eof
after 5000
puts "Download Complete !!!\r\n"
if [[file exists $config_file]] {
puts "Config File: $config_file downloaded successfully\r\n"
} else {
puts "ERROR: Config File: $config_file - Not Found\r\n"
if [[file exists $post_conf]]
{
puts "Post Config Script: $post_conf downloaded
successfully\r\n"
} else {
puts "ERROR: Post Config Script: $post_conf - Not Found\r\n"
}
Copy Config to Startup Config
print_f10do "show version"
after 5000
print_f10do "copy flash://$config_file startup-config"
print_f10do "yes"
after 5000
puts "Pre-Config Script Execution Successfull !!!\r\n"
exit 0

```

## Preconfiguration Script - BMP Mode

```
#!/usr/bin/expect

#/DELL-NETWORKING

Execute F10do and Print
proc print_f10do {cmd_str} {
 set str [exec f10do "$cmd_str"]
 set tmp_str [string map {\n \r\n} $str]
 puts $tmp_str
}

set ftp_ip "20.0.0.1"
set ftp_username "lab"
set ftp_passwd "lab"
set config_file "s4810-10-startup-config"
set post_conf "s4810-10-post-config.exp"
puts "Executing Pre-Config Script !!!!\r\n"
exec rm -rf "$config_file"
exec rm -rf "$post_conf"
puts "Downloading Startup Config and Post-Config
Script from $ftp_ip ...\r\n"
spawn ftp "$ftp_ip"
expect "Name .*: "
send "$ftp_username\r\n"
expect "Password: "
send "$ftp_passwd\r\n"
send "cd scripts\r\n"
expect "ftp>"
send "ls\r\n"
expect "ftp>"
send "get $post_conf\r\n"
expect "ftp>"
send "get $config_file\r\n"
expect "ftp>"
send "bye\r\n"
expect eof
after 5000
puts "Download Complete !!!!\r\n"
if {[file exists $config_file]} {
 puts "Config File: $config_file downloaded successfully\r\n"
} else {
 puts "ERROR: Config File: $config_file - Not Found\r\n"
}
if {[file exists $post_conf]} {
 puts "Post Config Script: $post_conf downloaded
successfully\r\n"
} else {
 puts "ERROR: Post Config Script: $post_conf - Not
Found\r\n"
}
Copy Config to Startup Config
print_f10do "show version"
after 5000
print_f10do "copy flash://$config_file startup-config"
print_f10do "yes"
after 5000
puts "Pre-Config Script Execution Successful
!!!!\r\n"
exit 0
```

## Post Configuration Script - BMP Mode

The following example shows an example of the post configuration script for the S4810 or S4820T platform:

```
#!/usr/bin/expect
#/DELL-NETWORKING
Post Config Script for S4810-10
Execute F10do and Print
proc print_f10do {cmd_str} {
set str [exec f10do "$cmd_str"]
set tmp_str [string map {\n \r\n} $str]
puts $tmp_str
}
Interfaces Configurations
set interface_list_slot [list "0/1" "0/5" "0/9"]
set interface_list [list "Te 0/1" "Te 0/5" "Te 0/9"]
set {remote_intf(Te 0/1)} "TenGigabitEthernet 0/1"
set {remote_intf(Te 0/5)} "TenGigabitEthernet 0/5"
set {remote_intf(Te 0/9)} "TenGigabitEthernet 0/9"
set hostname "S4810-10"
set max_min 10
set status_file "s4810-10-current-status.dat"
set ftp_ip "20.0.0.1"
puts [exec rstimer 30]
puts "\r\nReset Timer Complete\r\n"
Open Staus File
set fp [open $status_file w]
puts $fp "=====\r\n"
puts $fp " Status: $hostname\r\n"
puts $fp "=====\r\n"
Configure LLDP Protocol
puts "Configuring LLDP Protocol\r\n"
print_f10do "configure terminal"
print_f10do "protocol lldp"
print_f10do "no disable"
print_f10do "end"
Check for Protocl LLDP
set lldp_output [exec f10do "show runn | grep lldp"]
if {[regexp "lldp" $lldp_output]} {
puts "LLDP is configured\r\n"
Write the Result to Status File
puts $fp "LLDP is configured\n"
} else {
puts "ERROR: LLDP is not configured\r\n"
Write the Result to Status File
puts $fp "ERROR: LLDP is not configured\r\n"
}
Configure Interfaces
foreach intf_slot $interface_list_slot {
set intf "TenGigabitEthernet $intf_slot"
puts "Configuring $intf ... \n"
puts $fp "Configuring $intf ... \n"
print_f10do "configure terminal"
print_f10do "interface $intf"
print_f10do "no ip address"
print_f10do "no shutdown"
print_f10do "end"
after 200
}
Wait for 2 mins for the Neighbor to come-up
puts "Wait for 1 min for the Neighbor to come-up\r\n"
after [expr {60 * 1000}]
```

```

puts $fp "=====\n"
puts $fp " Checking Conectivity thru LLDP\n"
puts $fp "=====\n"
Check LLDP Configurations
foreach intf_slot $interface_list {
set min 0
set result 0
while {$result == 0 && $min < 5} {
set result_str [exec f10do "show lldp neighbors | grep
\"$intf_slot\""]
set tmp_str [string map {\n \r\n} $result_str]
puts $tmp_str
if {[regexp "$intf_slot" $result_str]} {
set result 1
if {[regexp "$remote_intf($intf_slot)" $result_str]} {
puts "Interface $intf_slot is Connected to
$remote_intf($intf_slot)\r\n"
puts $fp "Interface $intf_slot is Connected to
$remote_intf($intf_slot)\r\n"
} else {
puts "ERROR: Interface $intf_slot is Not Connected to Interface
$remote_intf($intf_slot)\r\n"
puts $fp "ERROR: Interface $intf_slot is Not Connected to
Interface$remote_intf($intf_slot) \r\n"
puts "LLDP Output for $intf_slot :\r\n $result_str \r\n"
puts $fp "LLDP Output for $intf_slot :\r\n $result_str \r\n"
}
}
continue
}
Wait for 1 minute
puts "Interface is Not Connected\r\n"
puts "Wait for 1 min for the Neighbor to come-up\r\n"
after [expr {60 * 1000}]incr min
}
if {$result == 1} {
puts "Interface $intf_slot is Connected\r\n"
Write Result to Status File
puts $fp "Interface $intf_slot is Connected\r\n"
} else {
puts "ERROR: Interface $intf_slot is Not Connected\r\n"
Write the Result to Status File
puts $fp "ERROR: Interface
$intf_slot is Not Connected\r\n"
}
}
Close & FTP Status File
puts $fp "=====\n"
close $fp
Configure FTP - Interface
print_f10do "configure terminal"
print_f10do "interface TenGigabitEthernet 0/22"
print_f10do "ip address 20.0.0.34/16"
print_f10do "no shutdown"
print_f10do "end"
puts "Uploading Status File($status_file) to $ftp_ip ... \n"
spawn ftp "$ftp_ip"
expect "Name .*: "
send "lab\n"
expect "Password:"
send "lab\n"
expect "ftp>"
send "cd scripts\n"
expect "ftp>"
send "ls\n"
expect "ftp>"
send "put $status_file\n"

```

```
expect "ftp>"
send "ls\n"
expect "ftp>"
send "bye\n"
expect eof
print_f10do "configure terminal"
print_f10do "interface TenGigabitEthernet 0/22"
print_f10do "no ip address"
print_f10do "shutdown"
print_f10do "end"
puts "Post-Config Script Execution Successfull !!!!!\r\n"
exit 0
```



# Bare Metal Provisioning (BMP)

## Overview

Bare Metal Provisioning (BMP) 3.0 is supported on the  **S4820T** , and MXL Switch platforms.



**Note:** Bare Metal Provisioning version 1.5 is supported on S55 and S60 platforms. For more information, refer to [Bare Metal Provisioning 1.5](#).

In a data center network, Bare Metal Provisioning (BMP) automates the configuration and updating of switches, ensuring standard configurations across installed devices.

To set up a single switch or a stack of switches with minimal effort, use the autoconfiguration function.

BMP eases configuration in the following key areas:


- On S4810, S4820T, Z9000, and MXL Switch platforms running BMP 3.0:
  - Boot images and running configurations are specified in a dynamic host configuration protocol (DHCP) server.
  - Configuration files are automatically downloaded from a file server and applied to the switch or stack.
  - Switch access is allowed through all ports (management and user ports) with or without DHCP-based dynamic IP address configuration of a switch.
  - Boots up in Layer 3 mode with interfaces already in No Shutdown mode and some basic protocols are enabled to protect the system and the network.
  - Supports pre-configuration and post-configuration scripts to automatically load predefined configurations and FTOS images using DHCP and common file transfer mechanisms.

## Commands

- [reload conditional nvram-cfg-change](#)
- [reload-type](#)
- [script post-config](#)

- [show boot bmp](#)
- [show reload-type](#)
- [stop bmp](#)
- [stop jump-start](#)

## reload conditional nvram-cfg-change

 **S4810**  
**S4820T**

MXL Switch

To perform a reload on the chassis to upgrade any configuration changes that have changed the NVRAM content, after saving the BMP configuration, use this command.

### Syntax

**reload conditional nvram-cfg-change**

### Defaults

None.

### Command Modes

EXEC

### Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *FTOS Command Line Reference Guide*.

---

Version 9.2(0.0) Introduced on the MXL Switch.

---

Version 9.1(0.0) Introduced on the Z9000 and S4810.

---

Version 8.3.19.0 Introduced on the S4820T.

---

### Usage Information

To upgrade any NVRAM changes to the chassis caused by the following CLI commands: **stack-unit {unit} stack-group**, **stack-unit {unit} port {fanout-portid} portmode quad**, **asf-mode**, **can-acl**, **buffer-profile**, use the **reload conditional nvram-cfg-change** command on a switch running BMP 3.0.

# reload-type

 **S4810**

**S4820T**

MXL Switch

Configure a switch to reload in normal mode or as a DHCP client with all ports configured for Layer 3 traffic.

## Syntax

**reload-type** {**normal—reload** | **bmp** [**auto—save** {**enable** | **disable**}] [**config-scr-download** {**enable** | **disable**}] [**dhcp-timeout** *minutes*]} [**retry-count** *number*] [**vendor-class-identifier** *description*]

To stop the BMP process, use the **stop bmp** command.

## Parameters

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>normal-reload</b>                              | Enable the normal reload type and disable BMP reload type. The system retrieves the FTOS image and startup-configuration files from the flash after performing a reload.                                                                                                                                                                                                                                                           |
| <b>bmp</b>                                        | (Default) Enable the BMP reload type. The system acts as a DHCP client and downloads the FTOS image and configuration file or script files from a specified DHCP server.                                                                                                                                                                                                                                                           |
| <b>auto-save</b>                                  | (Optional) Configure the <b>auto save</b> option to save the downloaded configuration or script file as they are not saved by default. When you configure auto save, downloaded configurations are automatically saved to the startup configuration. Auto saving the downloaded configurations also requires enabling the <b>config-scr-download</b> parameter. Downloaded scripts are automatically saved to the autoexec script. |
| <b>config-scr-download {enable}</b>               | (Optional) Configure whether the configuration file or preconfiguration script must be downloaded from the DHCP/file servers (enable).                                                                                                                                                                                                                                                                                             |
| <b>config-scr-download {disable}</b>              | (Optional) Configure if the downloaded file or preconfiguration script is not downloaded from the DHCP/file servers.                                                                                                                                                                                                                                                                                                               |
| <b>dhcp-timeout</b> <i>minutes</i>                | (Optional) Configure the DHCP timeout (in minutes) after which the BMP reload stops. The range is from 0 to 50. If you enter a range of 0, the timeout is 0 (no limit). The default is disabled.<br><b>Note:</b> Dell Networking recommends setting the value to 2 or higher.                                                                                                                                                      |
| <b>retry-count</b> <i>number</i>                  | Configure the number of times to retry loading the FTOS image and configuration or preconfiguration script download. The retry limit is from 0 to 6. If the retry limit is 0, no retry is performed. The default is 0.                                                                                                                                                                                                             |
| <b>vendor-class-identifier</b> <i>description</i> | (Optional) Enter a brief description for the user defined field in option 60. Maximum is 64 characters long.<br><b>Note:</b> This parameter replaces the deprecated <b>user-defined-string</b> parameter.                                                                                                                                                                                                                          |

## Defaults

BMP

Switches running BMP 3.0 reload in BMP mode as a DHCP client with all ports configured for Layer 3 traffic.

## Command Modes

CONFIGURATION

**Command History**

|                  |                                                                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version 9.2(0.0) | Introduced on the MXL Switch. Introduced support for <b>vendor-class-identifier</b> that replaces deprecated <b>user-defined-string</b> parameter. Also added support for <b>auto-save</b> and <b>retry-count</b> parameters.                        |
| Version 9.0(0.0) | Introduced on the Z9000. Updated the command mode from EXEC Privilege to GLOBAL CONFIGURATION. Updated the parameter from <b>jumpstart</b> to <b>bmp</b> . Added support for the <b>config-scr-download</b> and <b>user-defined-string</b> commands. |
| Version 8.3.19.0 | Introduced on the S4820T.                                                                                                                                                                                                                            |
| Version 8.3.1.0  | Introduced on the S4810.                                                                                                                                                                                                                             |

**Usage Information**

For an initial setup, the **config-scr-download** parameter of the **reload-type** command is enabled. After the configuration file is successfully downloaded, the **config-scr-download** parameter is automatically disabled. You can enable it again using the **reload-type** command.

Set the Auto Configuration mode (BMP or Normal reload) using the **reload-type** command. Next, enter the **reload** command to reload the switch in the configured mode.

When a switch reloads in BMP mode, all ports, including the management port, are automatically configured as Layer 3 physical ports. The switch runs the DHCP client on all interfaces. You can reconfigure the default startup configuration and DHCP timeout values.

If the switch attempts to contact a DHCP server and one is not found, it enters a loop while reloading in BMP mode. To interrupt the reload and boot up in Normal mode, enter the **stop bmp** command. The startup configuration is then loaded from the local flash on the switch.

To toggle between Normal and BMP Auto Configuration modes, use the **reload-type** command in BMP 3.0. Reload settings for Auto Configuration mode that you configure are stored in memory and retained for future reboots and BMP software upgrades. To reload the switch in the last configured mode, BMP or Normal reload mode, enter the **reload** command at any time.

Upgrade any configuration changes that have changed the NVRAM content by performing a reload on the chassis.


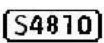
While BMP is on, the FTOS prompt changes to FTOS-BMP.

**Related Commands**

**show reload-type** — displays the current reload mode (BMP or Normal mode).

**stop bmp** — stops the BMP process and prevents a loop if the DHCP server is not found.

# script post-config

   
**S4820T**

To execute the post-configuration script after applying the startup configuration, run this command.

MXL Switch

**Syntax** `script post-config {script-name}`

|                   |                         |                                                                                               |
|-------------------|-------------------------|-----------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <code>scriptname</code> | Enter the name of the script to be run after the BMP start-up configuration has been applied. |
|-------------------|-------------------------|-----------------------------------------------------------------------------------------------|

**Defaults** None.

**Command Modes** CONFIGURATION

**Command History** This guide is platform-specific. For command information about other platforms, refer to the relevant *FTOS Command Line Reference Guide*.

---

Version 9.2(0.0) Introduced on the MXL Switch.

---

Version 9.1(0.0) Introduced on the Z9000 and S4810.


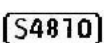
---

Version 8.3.19.0 Introduced on the S4820T.

---

**Usage Information** If a pre-configuration script for BMP 3.0 is executed and if the post configuration script is present in the start-up configuration, the post-configuration script executes.

# show boot bmp

   
**S4820T**

Displays the current state of the BMP process.

MXL Switch

**Syntax** `show boot bmp`

**Defaults** None.

**Command Modes** EXEC

|                        |                  |                                                         |
|------------------------|------------------|---------------------------------------------------------|
| <b>Command History</b> | Version 9.2(0.0) | Introduced on the Z9000, S4810, S4820T, and MXL Switch. |
|------------------------|------------------|---------------------------------------------------------|

**Example**

```

FTOS# show boot bmp
Config Download
via DHCP: enabled
BMP State : Waiting for boot options
...
BMP State : Received DHCP offer from DHCP server 25.1.1.1

***** SELECTED OFFER DETAILS *****
Server type= DHCP
Acquired IP= 25.1.1.25
Subnet-mask = 255.255.0.0
Image file = tftp://25.1.1.1/boot_file.bin
config file = tftp://25.1.1.1/config_file.cfg
Server IP = 25.1.1.1
TFTP Server IP = NIL
DNS IP = 25.1.1.1
Routers = NIL

...
BMP State : Downloading image boot_file.bin from 25.1.1.1

...
BMP State : Image boot_file.vin successfully downloaded

...
BMP State : BMP process is successfully completed

```

**Related  
Commands**

**reload-type** — Configures the reload mode as Normal or BMP.

## show reload-type

 **S4810**

**S4820T**

MXL Switch

Display the reload type currently configured on the system.

**Syntax**

**show reload-type**

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command  
History**

|                  |                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------|
| Version 9.2(0.0) | Introduced on the MXL Switch. Updated output example to include <b>auto-save</b> and <b>retry-count</b> parameters. |
| Version 9.1(0.0) | Updated <b>reload-type</b> parameters.                                                                              |
| Version 8.3.19.0 | Introduced on the S4820T.                                                                                           |
| Version 8.3.11.4 | Introduced on the Z9000.                                                                                            |
| Version 8.3.10.0 | Introduced on the S4810.                                                                                            |

**Usage  
Information**

Check the currently configured autoconfiguration mode (BMP or Normal reload) on a switch running BMP 3.0 using the **show reload-type** command.


To display the current reload mode for BMP 3.0, use the **show bootvar** or **show system brief** commands. The **show bootvar** command includes the path of the FTOS image file retrieved from a DHCP server when BMP is running, but not after you exit BMP.

**Example**

```
FTOS#show reload-type
Reload-Type : normal-reload [Next boot : bmp]
Auto-Save : enable
Config-Download : enable
Dhcp-Timeout : 30
Retry-Count : 4
```

**Related Commands**      **reload-type** — Configure the reload mode as BMP or Normal.

## stop bmp

 **S4810**

**S4820T**

MXL Switch

To prevent an infinite loop, stop the switch from reloading in BMP mode.

**Syntax**      **stop bmp**

**Note:** Replaces the **stop jumpstart** command.

**Defaults**      None.

**Command Modes**      EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant *FTOS Command Line Reference Guide*.

---

Version 9.2(0.0)    Introduced on the MXL Switch.

---

Version 9.1(0.0)    Introduced on the Z9000 and S4810. Replaces the **stop jumpstart** command.

---

Version 8.3.19.0    Introduced on the S4820T.

---

**Usage Information**

Use the **stop bmp** command on a switch running BMP 3.0 if the switch enters a loop while reloading in BMP mode. A loop occurs when the switch is continuously trying to contact a DHCP server and a DHCP server is not found. The **stop bmp** command stops the switch from connecting to the DHCP server. After you use the **stop bmp** command, the next default reload type is a normal reload as indicated in the **show reload-type** or **show system-brief** commands.

**Related Commands**      **reload-type** — Configures the reload mode as normal or BMP.

# stop jump-start

S55 S60 Z

S4810 S4820T

To prevent an infinite loop, stop the switch from reloading in BMP mode.

## Syntax

**stop jump-start**

**Note:** This command is deprecated on the S4810, S4820T, and Z9000 platforms. It is replaced by the **stop bmp** command.

## Defaults

None

## Command Modes

EXEC

## Command History

|                  |                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------|
| Version 9.1(0.0) | Deprecated command on the S4810, S4820T and Z9000 platforms. Replaced by the <b>stop bmp</b> command. |
| Version 8.3.19.0 | Introduced on the S4820T.                                                                             |
| Version 8.3.11.4 | Introduced on the Z9000.                                                                              |
| Version 8.3.10.1 | Introduced on the S4810.                                                                              |
| Version 8.3.5.0  | Introduced on the S55.                                                                                |
| Version 8.3.3.1  | Introduced on the S60.                                                                                |

## Usage Information

Use the **stop jump-start** command on a switch running BMP 2.0 if the switch enters a loop while reloading in Jumpstart mode. A loops occurs when the switch is continuously trying to contact a DHCP server and a DHCP server is not found. The **stop jump-start** command stops the switch from connecting to the DHCP server. The startup configuration file stored in the local flash on the switch is loaded as part of the **stop jump-start** command.

## Related Commands

**reload-type** — Configure the reload mode as Normal or Jumpstart (BMP).



# Smart Scripting

Smart Scripting is supported on the **S4810**, **S4820T**, Z9000, and the MXL Switch platforms.

Smart Scripting allows you to add functionality to the Dell Networking operating system (FTOS) without requiring updates to the FTOS release. Smart Scripting is available as a separate installable package that supports PERL, Python, and UNIX scripting and various FTOS functions.

The Smart Scripting package supports smart utility (SmartUtils) application programming interfaces (APIs) providing developers with an easier way to invoke switch operations by creating and running PERL, Python, and UNIX shell scripts on the FTOS operating system. API library files describe the functions supported in PERL, Python, and UNIX scripts.

A separate package has been extended with HTTP and HTTPS daemons based on CGI scripts and a Web-based graphical user interface. For more information on this package, see [Chapter 14, Web Server with HTTP Support](#). For information on the HTTP requests supported by the REST API, see [Chapter 13, Programmatic Interface REST API Commands](#).

## Overview

Using Smart Scripting, network administrators can create custom PERL, Python, and UNIX shell scripts to manage and interact with Dell Networking switches/routers in the network. Smart Scripting provides support for:

- Modules required to run PERL scripts, such as the software development kits (SDKs) for VMware and vCenter/vSphere.
- Modules that implement requested Python features, such as AMQP (message queuing), XML-RPC (arbitrary data exchange), and Twisted (event-driven networking engine).

With Smart Scripting, there is no need to learn proprietary scripting languages, allowing for the faster development and deployment of custom scripts.

Smart Scripting also offers solutions in a UNIX environment that are useful to cloud administrators who are familiar with working directly in a UNIX shell. Script support in a UNIX environment allows you to invoke standard UNIX utilities such as netstat, tcpdump, ls, chmod, chown, and so on.

Smart Scripting includes a convenient set of API function libraries to which script developers can refer when they create PERL, Python, and UNIX scripts. A representation of CLI functions to retrieve data from the FTOS operating system and change configuration parameters on Dell Networking switches is provided in the API libraries. Script writers include API function calls made directly on the FTOS command line interface (CLI) in their PERL, Python, and UNIX scripts.

For example, the API functions used in a script include setting up a telnet session, gathering data on the switch, sending information to the CLI, and closing telnet sessions. By using simple function calls, script writers do not have to include the parsing code required for telnet sessions and retrieving configuration information.

Smart Scripting supports running a script either from the FTOS CLI or directly from a UNIX shell. Run scripts periodically, based on events, at boot up or after the switch is initialized. You can run scripts in the foreground or background and display the progress of a script. If required, you can cancel, stop or resume scripts.

## Use Cases

Smart Scripting allows you to automate common management and maintenance tasks, such as:

- Building visibility and/or discovery programs.
- Creating custom logging.
- Reporting configuration information.
- Reporting switch memory usage, configured virtual local area networks (VLANs), and other operating and configuration parameters.
- Creating custom APIs for external applications to access the switch.
- Automating custom provisioning of network devices to support server virtualization.

For example, you can automate any of the following tasks:

- Monitor the configuration of switch ports to verify that no change occurs and generate an alarm if a configuration change is detected as part of a cloud-computing deployment.
- Stage CLI command requests received from a customer. If a link flaps, the command completion status is held in the script so you can see when the management plane reconnects.
- Generate time-based reports to receive updates on network status on a periodic basis.

- Query an external, configuration management database on a remote server to retrieve information on port operation, and reconfigure switch ports based on the data received.
- Apply additional time-based access-control lists (ACLs) to limit after hours access.
- Monitor network requests; for example, “find a specified MAC address” or “generate a health-check heartbeat”.
- Create a simple menu of options that a non-network administrator can use to create requests to be sent to the network.

Smart Scripting consolidates management data inside a switch and sends it to management consoles, databases, or applications – reducing polling and network traffic. For example, you can use a script as part of a cloud-computing deployment to detect when the network has changed, query a database server for Configuration Management Database (CMDB) information, and ultimately apply network changes based on the data.

## Downloading the Smart Scripting Package

Download the SmartScripts package from the Dell Networking website as a file named:

- **SMARTSCRIPTS2.0.0.tar.gz** file for S55, S60
- **SMARTSCRIPTS-P-3.0.0.0.tar.gz** for S4810 and S4820T
- **SMARTSCRIPTS-I-3.0.0.0.tar.gz** for Z9000
- **SMARTSCRIPTS-M-3.0.0.0.tar.gz** for MXL Switch

To download the SmartScripts package to a dedicated location (tftp, ftp, or flash), use one of the following methods:

The Smart Scripting package includes the following files and functionality:

- PERL interpreter and associated files
- Python interpreter and associated files
- Expanded set of UNIX utilities
- Web-Server with HTTP Support (see [Web Server with HTTP Support](#))

## Installing Smart Scripting

After you download the SmartScripts package, install the file from local flash memory on a switch or from an external drive on a network server. Because the installation takes time, it is performed in the background. When the download is complete, a message displays on the console. The package installation updates the running configuration file.

**CAUTION:**

You can modify (for example, edit or rename) the files downloaded with the Smart Scripting package only in the directory in which you install the package. Never modify the files in other system directories.

To install the Smart Scripting package, you must download it from the Dell Networking web portal:

1. On a PC or other network device, go to the Dell Networking web portal at <https://www.force10networks.com/CSPortal20/Main/SupportMain.aspx>. Click **Login**, enter your user ID and password, and click the **Login** button.
2. On the Customer Support page, click the **Software Center** tab.
3. In the left hand column, click **Automation Software**.
4. At the bottom of the Terms and Conditions page, click **I agree**.
5. On the Automation Software page, under Software, select the file for the switch from the following list:
  - **SMARTSCRIPTS2.0.x.tar.gz** file for S55 and S60
  - **SMARTSCRIPTS-P-3.0.0.0.tar.gz** for S4810 and S4820T
  - **SMARTSCRIPTS-I-3.0.0.0.tar.gz** for Z9000
  - **SMARTSCRIPTS-M-3.0.0.0.tar.gz** for MXL Switch
6. In the dialog box, select the path for the local flash on the switch or a directory path on a network server where you want to download the **SMARTSCRIPTS** file for your switch.

- When the download is complete, enter the **package install** command from the FTOS CLI on a switch to install the Smart Scripting package.

| Command Syntax                                                                                                                                                                                                                                                                                                                                                                                         | Command Mode   | Task                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>package install</b> { <b>flash://filename</b>   <b>ftp://userid:password@host-ipaddress/dir-path</b>   <b>tftp://host-ipaddress/dir-path</b> }                                                                                                                                                                                                                                                      | EXEC Privilege | Install the Smart Scripting package from local flash memory or a network server to a dedicated location on your server for script storage. |
| Where:                                                                                                                                                                                                                                                                                                                                                                                                 |                |                                                                                                                                            |
| <ul style="list-style-type: none"> <li><b>flash://filename</b> installs the Smart Scripting file stored in flash memory on the switch.</li> <li><b>ftp://userid:password@host-ipaddress/filepath</b> logs in and installs Smart Scripting from a file stored on an FTP server.</li> <li><b>tftp://host-ipaddress/filepath</b> installs Smart Scripting from a file stored on a TFTP server.</li> </ul> |                |                                                                                                                                            |

To remove an installed Open Automation package, such as Smart Scripting, enter the **package uninstall** command.

To follow the progress of a package installation (or removal), enter the **show packages** command.

## Displaying Installed Packages

To view the Open Automation packages currently installed on a switch, including version numbers and content, enter the **show packages** command.

| Command Syntax       | Command Mode   | Task                      |
|----------------------|----------------|---------------------------|
| <b>show packages</b> | EXEC Privilege | View package information. |

## Uninstalling Smart Scripting



**Caution:** Before you uninstall the Smart Scripting package, you must first stop all scripts that are currently running using the **no script *script-name*** command. You must also manually stop the http server daemon.



**Note:** If installed, uninstall the VSN Agent package before uninstalling Smart Scripting package.

Uninstalling the Smart Scripting package removes it from the internal flash memory.

| Command Syntax                                                                                                                                         | Command Mode   | Task                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------------------------------------------------------|
| <b>package uninstall</b> <i>package-name</i><br>Enter the name of the Smart Scripting package, exactly as it appears in the <b>show packages</b> list. | EXEC Privilege | Uninstall the Smart Scripting package stored on the switch. |

## Limits on System Usage

Smart Scripting establishes limits on system processes for the following attributes (regardless of the user-privilege level or scripting method) to restrict CPU and memory usage:

**Table 7-1. Limits on System Attributes**

| System Attribute | Value     | Description                                                                                                                                                                                                                                                                              |
|------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cputime          | unlimited | Maximum amount of time used by a process.                                                                                                                                                                                                                                                |
| filesize         | unlimited | Largest file size (in bytes) that can be created.                                                                                                                                                                                                                                        |
| datasize         | 131,072   | Maximum size (in bytes) of the data segment for a process; this value defines how far a program may extend its break with the <code>sbrk(2)</code> system call.                                                                                                                          |
| stacksize        | 2,048     | Maximum size (in bytes) of the stack segment for a process; this value defines how far a program's stack segment may be extended. Stack extension is performed automatically by the system.                                                                                              |
| coredumpsize     | unlimited | Largest size (in bytes) of a core file that may be created                                                                                                                                                                                                                               |
| memory use       | 233,244   | Maximum size (in bytes) to which a process's resident set size may grow. This value imposes a limit on the amount of physical memory to be given to a process; if memory is tight, the system prefers to take memory from processes that are exceeding their declared resident set size. |
| memorylocked     | 77,741    | Maximum size (in bytes) which a process may lock into memory using the <code>mlock(2)</code> function.                                                                                                                                                                                   |

**Table 7-1. Limits on System Attributes**

| System Attribute | Value | Description                                                       |
|------------------|-------|-------------------------------------------------------------------|
| maxproc          | 160   | Maximum number of simultaneous processes allowed for the user ID. |
| openfiles        | 64    | Maximum number of open files for this process.                    |

## Supported UNIX Utilities

Smart Scripting supports the invocation of the following UNIX utilities in the scripts you run:

**Table 7-2. Supported UNIX Utilities**

| UNIX Utility | Function                                          |
|--------------|---------------------------------------------------|
| arp          | Address resolution display and control.           |
| awk          | Pattern scanning and processing language.         |
| basename     | Return filename or directory portion of pathname. |
| bc           | An arbitrary precision calculator language.       |
| cat          | Concatenate and print files.                      |
| chmod        | Change file modes.                                |
| chown        | Change file owner and group.                      |
| cksum        | Display file checksums and block counts.          |
| cut          | Select portions of each line of a file.           |
| date         | Display or set date and time.                     |
| dd           | Convert and copy a file.                          |
| df           | Display free disk space.                          |
| env          | Set and print environment.                        |
| expr         | Evaluate expression.                              |
| fc           | List the history of commands on the computer.     |
| fg           | Change the background process to foreground.      |
| file         | Determine file type.                              |
| find         | Walk a file hierarchy.                            |
| ftp          | Internet file transfer program.                   |
| getopts      | Called each time you want to process an argument. |
| grep         | Print lines matching a pattern.                   |
| hostname     | Set or print name of current host system.         |
| ifconfig     | Configure network interface parameters.           |
| iostat       | Report I/O statistics.                            |
| ln           | Make links.                                       |

**Table 7-2. Supported UNIX Utilities (continued)**

|         |                                                             |
|---------|-------------------------------------------------------------|
| ls      | List directory contents.                                    |
| md5     | Calculates and verifies 128-bit MD5 hashes.                 |
| more    | A filter for browsing text files.                           |
| netstat | Show network status                                         |
| nice    | Execute a utility with an altered scheduling priority.      |
| nohup   | Invoke a command immune to hangups.                         |
| ping    | Send ICMP ECHO_REQUEST packets to network hosts.            |
| ps      | Process status.                                             |
| pwd     | Return working directory name.                              |
| sed     | Stream editor.                                              |
| sleep   | Suspend execution for an interval of time.                  |
| sort    | Sort or merge text files.                                   |
| ssh     | Open SSH client (remote login program).                     |
| stty    | Used for changing the settings of a UNIX computer terminal. |
| tail    | Display the last part of a file.                            |
| test    | Condition evaluation utility.                               |
| ulimit  | Get and set process limits.                                 |
| umask   | Set file creation mode mask.                                |
| vmstat  | Report virtual memory statistics.                           |
| wait    | Await process completion.                                   |
| wc      | Word, line, and byte count.                                 |
| who     | Display the users who are currently logged in.              |

## Creating PERL, Python, and UNIX Scripts

When you install the Smart Scripting package, sample PERL and Python scripts are installed in the `/usr/pkg/scripts/sample_scripts` directory. You can also create your own customized scripts and store them anywhere on the switch, such as in a `/f10/flash_scripts` directory.

In addition, you can use the PERL, Python, and UNIX APIs to create scripts that invoke function calls directly in the FTOS CLI. These APIs provide a shortcut when writing scripts. For more information, refer to the following sections:

- [Using the PERL API](#)
- [Using the Python API](#)
- [Using UNIX Shell Scripting](#)

For instructions about how to run a PERL, Python, or UNIX script from the FTOS CLI, refer to [Running Scripts with User Privileges](#).



For information about how to run a PERL, Python, or UNIX script directly from a UNIX shell, refer to [Running a Script from the UNIX Shell](#).

## Creating a User Name and Password for Smart Scripting

Before you run a script from the FTOS CLI, you may want to configure an additional user name and password to be used only to run scripts on a switch. Use the user name and password to log into a UNIX shell and apply the read-write privileges assigned to the user name when a script is run with the **script** command from the FTOS CLI.

The user name is an optional entry in the **script** command (refer to [Running Scripts with User Privileges](#)). To satisfy the requirements for a UNIX BSD login, the username must be less than 16 characters. A username used to run scripts cannot contain special characters.

| Command Syntax                                              | Command Mode  | Task                                                                                                                                 |
|-------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>username</b> <i>name</i> <b>password</b> <i>password</i> | CONFIGURATION | Create an additional user name and password that are used to log in to a shell and apply read-write privileges when a script is run. |

## Downloading Scripts to a Switch

Download a script to the switch using TFTP, FTP, or FLASH. Save the script to the dedicated script storage location, /usr/pkg/ss-scripts.

| Command Syntax                                                                                                                                            | Command Mode  | Task                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mount nfs</b> <i>nfs-server-ip:</i><br><b>remote_dir</b> <b>mount_name</b><br>[ <b>username</b> <i>username</i>  <br><b>password</b> <i>password</i> ] | CONFIGURATION | Configure the folders to mount a remote directory in the local FTOS path through a network file system (NFS). Enter the name of the remote directory to be mounted through the network file system or the name of the folder in the local system. |
| <b>script get url</b>                                                                                                                                     | EXEC          | Copy a script to a switch. Downloaded files are stored in a dedicated folder.                                                                                                                                                                     |
| <b>script remove</b> { <b>file_name</b><br><i>file-name</i>   <b>all</b> }                                                                                | EXEC          | Remove a script from a switch.                                                                                                                                                                                                                    |

## Setting a Search Path for Scripts

Create a path to the location where scripts are stored to be used by FTOS when searching for scripts. This negates the need to specify a specific path when executing a script.

| Command Syntax                      | Command Mode  | Task                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>script path</b> <i>path-name</i> | CONFIGURATION | Set a search path for a script in FTOS. The script path can contain a network file system mounted directory (defined in the <b>mount nfs</b> command). The path is added to a script search list allowing the system to search all locations for the script name. If the script is in multiple locations, the system uses the first instance of the script found. |

## Running Scripts with User Privileges

Administer any PERL, Python, and UNIX shell script stored on the switch from the FTOS CLI.

When running a script from the FTOS CLI, specify an optional user name to apply the associated read-write privileges when the script is run (refer to [Creating a User Name and Password for Smart Scripting](#)). If you do not specify a user name, the script runs with the privileges of the current user.

To run a PERL, Python, or UNIX script from the FTOS CLI, enter the **script** command. Enter the script name and directory path to start the script. The script can invoke any of the supported UNIX utilities listed in [Table 7-2](#). Enter the command multiple times to run more than one script at the same time.

| Command Syntax                                                                                                                | Command Mode  | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>script</b> [ <b>username</b> <i>name</i> ]<br><i>script-path</i> [ <i>script-parameter</i><br><i>script-parameter</i> ...] | CONFIGURATION | Run an installed script; for examples refer to <a href="#">Figure 7-2</a> . For <i>script-path</i> , enter the directory path and filename. (Optional) For <b>username</b> <i>name</i> , enter the user name whose read-write privileges are applied when the script runs. A username used to run scripts cannot contain special characters. (Optional) For <i>script-parameter</i> , enter the values of up to three parameters to be applied when the script runs. Enter a blank space between parameter values; for example:<br><b>script username admin /f10/flash/createVlans.py 1 2</b> |

# Scheduling Time / Event-based Scripts

Schedule scripts to execute periodically, based on an event, at a specific time, at boot up, or after you configure the switch. Manage scripts to stop executing after a set period of time or configured to run at optimal times for critical resources such as switch CPU load or packet loss.

## Triggering a Script to Run

To trigger scripts to run periodically or based on an event, use the following commands.

| Command Syntax                                                                                                                                                                                                                                                                                                           | Command Mode  | Task                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schedule a script to run in EXEC mode.                                                                                                                                                                                                                                                                                   |               |                                                                                                                                                                                                                       |
| <b>script execute</b> <i>script-name</i> <b>start</b> { <b>now</b>   <i>time-date</i>   <i>time</i> } [ <b>stop</b> { <b>at</b> <i>time-date</i>   <b>after</b> <i>time</i> }] [ <b>args</b> <i>arguments</i> ] [ <b>bg</b> ]                                                                                            | EXEC          | Schedule a script to execute at a specific time and optionally stop after a specified time. By default, the script runs in the foreground. To run the script in the background, use the <b>bg</b> parameter.          |
| <pre>FTOS#script execute hello.txt start now stop after 00:20 args "hi" FTOS#script execute sample.zsh start 01:12 bg</pre>                                                                                                                                                                                              |               |                                                                                                                                                                                                                       |
| Define a trigger event.                                                                                                                                                                                                                                                                                                  |               |                                                                                                                                                                                                                       |
| <b>script trigger-event</b> <i>event-name</i> { <b>log-event</b> { <b>tag</b> <i>tag</i> }   <b>severity</b> <i>severity level</i> }   <b>time-event</b> <i>time</i>   <b>cpu-usage</b> <i>percentage</i>   <b>mem-usage</b> <i>percentage</i> }                                                                         | CONFIGURATION | Define an event to use to trigger scripts to run by a log event (for example, SYSLOG in FTOS), a time-based event or when CPU or memory usage reaches a pre-determined percentage. The script runs in the background. |
| <pre>FTOS(conf)#script trigger-event event1 log-event tag "OSTATE_UP"</pre>                                                                                                                                                                                                                                              |               |                                                                                                                                                                                                                       |
| Schedule a script to run based on defined events.                                                                                                                                                                                                                                                                        |               |                                                                                                                                                                                                                       |
| <b>script execute</b> <i>script-name</i> <b>triggered-by</b> <i>event-name</i> [ <b>args</b> <i>arguments</i> ]                                                                                                                                                                                                          | CONFIGURATION | Schedule a script to run triggered by a defined trigger event.                                                                                                                                                        |
| <pre>FTOS(conf)#script execute sample.pl triggered-by event1 args "hi"</pre> <p>Where event 1 is defined by a trigger event.</p>                                                                                                                                                                                         |               |                                                                                                                                                                                                                       |
| Schedule a script to run periodically.                                                                                                                                                                                                                                                                                   |               |                                                                                                                                                                                                                       |
| <b>script execute</b> <i>script-name</i> <b>start</b> { <b>now</b>   <i>time-date</i>   <i>time</i> } <b>repeat</b> { <b>weekdays</b> <i>weekday</i>   <b>days</b> <i>day</i>   <b>minutes</b> <i>minutes</i> } [ <b>stop</b> { <b>at</b> <i>time-date</i>   <b>after</b> <i>time</i> }] [ <b>args</b> <i>argument</i> ] | CONFIGURATION | Schedule scripts to run at a certain time, to be repeated, or to stop at a specified time or by a string of arguments. The script runs in the background.                                                             |
| <pre>FTOS(conf)#script execute sample.tcl repeat weekday all args "sample-script"</pre>                                                                                                                                                                                                                                  |               |                                                                                                                                                                                                                       |

| Command Syntax                                                               | Command Mode  | Task                                                                                                                           |
|------------------------------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| Assign scripts to execute on boot up                                         |               |                                                                                                                                |
| <b>script list execute</b> <i>list-name</i><br><b>{on-boot   network-up}</b> | CONFIGURATION | Assign the order and run levels to a list of boot scripts to execute on boot up or after the switch is completely initialized. |
| FTOS(conf)#script list execute list on-boot                                  |               |                                                                                                                                |

## Managing Executed Scripts

Manage scripts to run at optimal times, view a list of scripts currently running, or stop, resume, or cancel a script from running using the following commands.

Protect system resources by scheduling scripts to run when resources are within configured threshold parameters. System resources include switch CPU, memory, and file system.

```
FTOS#show script process detail

JobID Script Type Script Status Script Name Args

000 TRIGGER Running admin.pl
001 REPEAT Running sample.zsh
FTOS#
```

To stop a currently running script, enter the **script stop** command.

```
FTOS#script stop script-name admin.pl
```

To resume running a script that has been stopped, enter the **script resume** command.

```
FTOS#script resume job-id 0
```

To kill a script that is running, enter the **script kill** command.

```
FTOS#script kill script-name admin.pl
```

```
FTOS#script kill all
```

To display scripts that are currently running, including the scripts you have stopped, enter the **show running-config | grep** command.

**Tip:** For information about running a script directly from a UNIX shell without using the FTOS CLI, refer to [Running a Script from the UNIX Shell](#).

## Viewing Script Information

To view information on currently stored, scheduled, and running SmartScripts, enter the following **show** commands.

| Command Syntax                      | Command Mode   | Task                                                                                                              |
|-------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------|
| <b>show script file [detail]</b>    | EXEC Privilege | Display the list of stored files in the script path. Enter <b>detail</b> to show the detail output of the file.   |
| <b>show script process [detail]</b> | EXEC Privilege | Display list of scripts that are scheduled or running. Enter <b>detail</b> to show the detail output of the file. |

## Logging in to a NetBSD UNIX Shell

To log into the NetBSD UNIX shell on a switch to directly enter any of the UNIX commands described in [Table 7-2](#) or to run a script, enter the **start shell** command. You are prompted to enter a user name and password before you can access the shell. Login is performed using SSHv2.

| Command Syntax     | Command Mode   | Task                                                                                                                |
|--------------------|----------------|---------------------------------------------------------------------------------------------------------------------|
| <b>start shell</b> | EXEC Privilege | Access the shell to run UNIX commands or a script (refer to <a href="#">Running a Script from the UNIX Shell</a> ). |

## Running a Script from the UNIX Shell

You can run any PERL, Python, and UNIX script stored on a switch from either the FTOS CLI (refer to [Running Scripts with User Privileges](#)) or directly from a NetBSD shell on the switch.

When you run a script from a UNIX shell, you must first access the shell by entering the **start shell** command (refer to [Logging in to a NetBSD UNIX Shell](#)). You are prompted to enter a user name and password configured with the **username** command (refer to [Creating a User Name and Password for Smart Scripting](#)).

[Figure 7-1](#) shows examples of how to execute a PERL, Python, and UNIX shell script directly from a NetBSD shell on FTOS.

**Figure 7-1. Execution of a PERL, Python, and Shell Script from a UNIX Shell: Example**

```

FTOS# start shell <----- Log on to a UNIX shell

4.4 BSD UNIX () (tty0)

login: admin
Password:
Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002
 The NetBSD Foundation, Inc. All rights reserved.
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
 The Regents of the University of California. All rights reserved.

$ cd /f10/flash/scripts
$ ls <----- List the existing scripts
createVlans.pl createVlans.py createVlans.sh

$./createVlans.pl 12 14 <----- Execute the PERL script using either command
$ perl createVlans.pl 12 14

$./createVlans.py 12 14 <----- Execute the Python script using either command
$ python createVlans.py 12 14

$./createVlans.sh 12 14 <----- Execute the UNIX shell script

```

## Using the PERL API

To create a PERL script using the PERL API and run the script on a Dell Networking switch, use the information in this section. For information about creating and running a Python script using the Python API, refer to [Using the Python API](#).

### Creating a PERL API Script

The Programmatic Interface package provides a PERL API library containing the supported functions (described in [Table 7-2](#)), which you can use in a PERL script to invoke FTOS operations on a switch. The PERL API library is stored in the FIOSmartUtils.pl file at /usr/pkg/scripts/smartutils.

Code FTOS API functions in a PERL script as shown in the following example:

**Figure 7-2. PERL Script with API function call: Example**

```
#!/usr/pkg/bin/perl -w

require '/usr/pkg/scripts/smartutils/F10SmartUtils.pl'; <----- Load the PERL API

usage() if ($#ARGV < 1);
($start,$end)=@ARGV;

$startVlan = $start;
$endVlan = $end;

for (my $i=$startVlan;$i<=$endVlan;$i++) {
 my $createvlanId = F10CreateVlanId($i); <----- Invoke a PERL API function
}

sub usage {
 print "usage: createVlans.pl <start> <end>\n";
 exit;
}
```

Table 7-2 describes the supported functions and required arguments that you can use in PERL scripts running on a Dell Networking switch to connect through a telnet session and gather information or configure parameters through the CLI.

**Table 7-3. Supported FTOS API Functions in PERL Scripts**

| PERL API Function        | Arguments                               | Description                                                                                                   |
|--------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------|
| F10AddLagIntToVlan       | (lagId, vlanId, tagFlag)                | Adds a LAG interface to a VLAN as either tagged or untagged. tagFlag values: 1 (tagged) or 0 (untagged).      |
| F10AddPhyIntToVlan       | (stackUnitNum, portId, vlanId, tagFlag) | Adds a physical interface to a VLAN as either tagged or untagged. tagFlag values: 1 (tagged) or 0 (untagged). |
| F10CreateVlanId          | (vlanId)                                | Creates a VLAN on the switch.                                                                                 |
| F10DeleteVlanId          | (vlanId)                                | Deletes a VLAN on the switch.                                                                                 |
| F10ExecShowCmd           | (command)                               | Executes a specified <b>show</b> command.                                                                     |
| F10MakeLagIntNoShutdown  | (lagId)                                 | Enables the specified port channel.                                                                           |
| F10MakeLagIntShutdown    | (lagId)                                 | Disables the specified port channel.                                                                          |
| F10MakeLagIntSwitch      | (lagId)                                 | Configures the specified port channel (LAG) as a Layer 2 switchport.                                          |
| F10MakePhyIntNoShutdown  | (stackUnitNum, portId)                  | Enables the specified port.                                                                                   |
| F10MakePhyIntShutdown    | (stackUnitNum, portId)                  | Disables the specified port.                                                                                  |
| F10MakePhyIntSwitch      | (stackUnitNum, portId)                  | Configures the specified port as a Layer 2 switchport.                                                        |
| F10MakeVlanIntNoShutdown | (vlanId)                                | Enables the specified VLAN interface.                                                                         |
| F10MakeVlanIntShutdown   | (vlanId)                                | Disables the specified VLAN interface.                                                                        |

**Table 7-3. Supported FTOS API Functions in PERL Scripts (continued)**

|                          |                        |                                                                                         |
|--------------------------|------------------------|-----------------------------------------------------------------------------------------|
| F10Ping                  | (ipAddress)            | Pings (via ICMP) an IP address from the switch.                                         |
| F10ShowArpTbl            | None                   | Returns the table of learned ARP entries.                                               |
| F10ShowBGPNeighbors      | None                   | Returns list of BGP neighbors.                                                          |
| F10ShowBGPRoute          | None                   | Returns the table of BGP-learned routes.                                                |
| F10ShowBGPSummary        | None                   | Returns summary information on BGP sessions.                                            |
| F10ShowBootVar           | None                   | Returns system boot variables.                                                          |
| F10ShowEnvironment       | None                   | Returns environment-monitoring variable values.                                         |
| F10ShowIntBrief          | None                   | Returns brief interface status (up/down/admin up/admin down) of all interfaces.         |
| F10ShowIntBriefLag       | None                   | Returns brief interface status (up/down/ admin up/down) of all port-channel interfaces. |
| F10ShowIntBriefMan       | None                   | Returns brief interface status (up/down/ admin up/down) of all management interfaces.   |
| F10ShowIntBriefPhy       | None                   | Returns brief interface status (up/down/ admin up/down) of all physical interfaces.     |
| F10ShowIntBriefVlan      | None                   | Returns brief interface status (up/down/ admin up/down) of all VLAN interfaces.         |
| F10ShowIPRoute           | None                   | Returns routing table information.                                                      |
| F10ShowISISNeighbors     | None                   | Returns list of ISIS neighbors.                                                         |
| F10ShowISISRoute         | None                   | Returns the table of ISIS-learned routes.                                               |
| F10ShowLagIntStatus      | (lagId)                | Returns the detailed status of a specified port-channel interface.                      |
| F10ShowLagIntVlanMembers | (lagId)                | Returns information on VLAN membership for a specified port-channel interface.          |
| F10ShowLog               | None                   | Returns the switch log buffer.                                                          |
| F10ShowMacAddrTbl        | None                   | Returns the table of learned MAC addresses.                                             |
| F10ShowMem               | (lagId)                | Returns switch memory usage.                                                            |
| F10ShowOSPFNeighbors     | None                   | Returns list of OSPF neighbors.                                                         |
| F10ShowOSPFRoute         | None                   | Returns the table of OSPF-learned routes.                                               |
| F10ShowPhyIntBand        | (stackUnitNum, portId) | Returns in/out bandwidth average for a specified port.                                  |
| F10ShowPhyIntStatus      | (stackUnitNum, portId) | Returns the detailed status of a specified physical interface.                          |
| F10ShowPhyIntVlanMembers | (stackUnitNum, portId) | Returns information on VLAN membership for a specified physical interface.              |
| F10ShowProcCpu           | None                   | Returns switch CPU usage and running processes.                                         |
| F10ShowRun               | None                   | Returns the running configuration (in memory).                                          |
| F10ShowVer               | None                   | Returns software version information.                                                   |
| F10ShowVlan              | None                   | Returns the <b>show vlan</b> output for all VLANs.                                      |
| F10ShowVlanId            | (vlanId)               | Returns the <b>show vlan</b> output for a specific vlan.                                |
| F10ShowVlanIntStatus     | (vlanId)               | Returns the detailed status of a specified VLAN interface.                              |
| F10ShowVrrp              | None                   | Returns the full VRRP status output.                                                    |



**Table 7-3. Supported FTOS API Functions in PERL Scripts (continued)**

|                  |                      |                                                                    |
|------------------|----------------------|--------------------------------------------------------------------|
| F10ShowVrrpBrief | None                 | Returns a brief VRRP session summary.                              |
| F10Traceroute    | (ipAddress, timeout) | Performs a traceroute operation to an IP address from the switch.  |
| F10WriteMem      | None                 | Write the running configuration to the startup configuration file. |

## Running a PERL API Script

When you run a PERL script that invokes the API functions in [Table 7-2](#), logon credentials are read from the smartutils.cfg file, and a telnet session opens on the switch in which function calls are executed in the FTOS CLI. The script closes the telnet session after running all the CLI commands.

The smartutils.cfg file is the configuration file used by the Programmatic Interface package. It contains the user name and passwords required to log on to a switch via telnet and access the CLI to execute the function calls in a PERL API script. The smartutils.cfg file downloads with the Programmatic Interface package and is stored at /usr/pkg/scripts/smartutils.



**Note:** Use the user name and passwords contained in the smartutils.cfg file to log in and run only the scripts created using the PERL, Python, and UNIX APIs described in this chapter. A username used to run scripts cannot contain special characters.

To configure the username and passwords located in the smartutils.cfg file that are used to run PERL API scripts, do one of the following:

- From a UNIX shell, use the UNIX text editor to open the smartutils.cfg file, enter a user name and password, and save the file.

To run a PERL API script:

- From the FTOS CLI, use the **script** command as described in [Running Scripts with User Privileges](#).
- From a UNIX shell, follow the procedure described in [Running a Script from the UNIX Shell](#).

## Using the Python API

To create a Python script using the Python API and run the script on a Dell Networking switch, use the information in this section. For information about creating and running a PERL script using the PERL API, refer to [Supported UNIX Utilities](#).

## Creating a Python API Script

To create a Python script to be run on a Dell Networking switch, use the information in this section. For information about how to run a Python script from the FTOS CLI, refer to [Running Scripts with User Privileges](#).

F10SmartUtils.py is the Python API library containing the supported functions (described in [Table 7-4](#)), which you can use in a Python script to invoke FTOS operations on a switch. This file is stored at /usr/pkg/scripts/smartutils.

Code FTOS API functions in a Python script as shown in the following example:

**Figure 7-3. Python Script with API function call: Example**

```
#!/usr/pkg/bin/python

import sys

sys.path.append('/usr/pkg/scripts/smartutils') <----- Load the Python
API

import F10SmartUtils

def create_vlans(startId,endId):
 for vlanId in range(startId,endId+1):
 result = F10SmartUtils.F10CreateVlanId(vlanId) <----- Invoke a Python API
function
 print result

def main(args):
 try:
 startId = int(args[0])
 endId = int(args[1])
 if(startId<=endId):
 create_vlans(startId, endId)
 else :
 print "Invalid range: startId cannot be larger than
endId",startId,endId
 except ValueError:
 print "Invalid arguments",args

if __name__=="__main__":
 if len(sys.argv)>2:
 main(sys.argv[1:])
 else:
 print "Please supply valid arguments"
 print "createVlans.py <startId> <endId>"
```

Table 7-4 describes the supported functions and required arguments that you can use in Python scripts running on a Dell Networking switch to connect through a telnet session and gather information or configure parameters through the CLI.

**Table 7-4. Supported FTOS API Functions in Python Scripts**

| Python API Function      | Arguments                               | Description                                                                                                   |
|--------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------|
| F10AddLagIntoVlan        | (lagId, vlanId, tagFlag)                | Adds a LAG interface to a VLAN as either tagged or untagged. tagFlag values: 1 (tagged) or 0 (untagged).      |
| F10AddPhyIntoVlan        | (stackUnitNum, portId, vlanId, tagFlag) | Adds a physical interface to a VLAN as either tagged or untagged. tagFlag values: 1 (tagged) or 0 (untagged). |
| F10CreateVlanId          | (vlanId)                                | Creates a VLAN on the switch.                                                                                 |
| F10DeleteVlanId          | (vlanId)                                | Deletes a VLAN on the switch.                                                                                 |
| F10ExecShowCmd           | (command)                               | Executes a specified <b>show</b> command.                                                                     |
| F10MakeLagIntNoShutdown  | (lagId)                                 | Enables the specified port channel.                                                                           |
| F10MakeLagIntShutdown    | (lagId)                                 | Disables the specified port channel.                                                                          |
| F10MakeLagIntSwitch      | (lagId)                                 | Configures the specified port channel (LAG) as a Layer 2 switchport.                                          |
| F10MakePhyIntNoShutdown  | (stackUnitNum, portId)                  | Enables the specified port.                                                                                   |
| F10MakePhyIntShutdown    | (stackUnitNum, portId)                  | Disables the specified port.                                                                                  |
| F10MakePhyIntSwitch      | (stackUnitNum, portId)                  | Configures the specified port as a Layer 2 switchport.                                                        |
| F10MakeVlanIntNoShutdown | (vlanId)                                | Enables the specified VLAN interface.                                                                         |
| F10MakeVlanIntShutdown   | (vlanId)                                | Disables the specified VLAN interface.                                                                        |
| F10Ping                  | (ipAddress)                             | Pings (via ICMP) an IP address from the switch.                                                               |
| F10ShowArpTbl            | None                                    | Returns the table of learned ARP entries.                                                                     |
| F10ShowBGPNeighbors      | None                                    | Returns list of BGP neighbors.                                                                                |
| F10ShowBGPRoute          | None                                    | Returns the table of BGP-learned routes.                                                                      |
| F10ShowBGPSummary        | None                                    | Returns summary information on BGP sessions.                                                                  |
| F10ShowBootVar           | None                                    | Returns system boot variables.                                                                                |
| F10ShowEnvironment       | None                                    | Returns environment-monitoring variable values.                                                               |
| F10ShowIntBrief          | None                                    | Returns brief interface status (up/down/admin up/admin down) of all interfaces.                               |
| F10ShowIntBriefLag       | None                                    | Returns brief interface status (up/down/ admin up/down) of all port-channel interfaces.                       |
| F10ShowIntBriefMan       | None                                    | Returns brief interface status (up/down/ admin up/down) of all management interfaces.                         |
| F10ShowIntBriefPhy       | None                                    | Returns brief interface status (up/down/ admin up/down) of all physical interfaces.                           |
| F10ShowIntBriefVlan      | None                                    | Returns brief interface status (up/down/ admin up/down) of all VLAN interfaces.                               |
| F10ShowIPRoute           | None                                    | Returns routing table information.                                                                            |

**Table 7-4. Supported FTOS API Functions in Python Scripts (continued)**

|                          |                        |                                                                                |
|--------------------------|------------------------|--------------------------------------------------------------------------------|
| F10ShowISISNeighbors     | None                   | Returns list of ISIS neighbors.                                                |
| F10ShowISISRoute         | None                   | Returns the table of ISIS-learned routes.                                      |
| F10ShowLagIntStatus      | (lagId)                | Returns the detailed status of a specified port-channel interface.             |
| F10ShowLagIntVlanMembers | (lagId)                | Returns information on VLAN membership for a specified port-channel interface. |
| F10ShowLog               | None                   | Returns the switch log buffer.                                                 |
| F10ShowMacAddrTbl        | None                   | Returns the table of learned MAC addresses.                                    |
| F10ShowMem               | (lagId)                | Returns switch memory usage.                                                   |
| F10ShowOSPFNeighbors     | None                   | Returns list of OSPF neighbors.                                                |
| F10ShowOSPFRoute         | None                   | Returns the table of OSPF-learned routes.                                      |
| F10ShowPhyIntBand        | (stackUnitNum, portId) | Returns in/out bandwidth average for a specified port.                         |
| F10ShowPhyIntStatus      | (stackUnitNum, portId) | Returns the detailed status of a specified physical interface.                 |
| F10ShowPhyIntVlanMembers | (stackUnitNum, portId) | Returns information on VLAN membership for a specified physical interface.     |
| F10ShowProcCpu           | None                   | Returns switch CPU usage and running processes.                                |
| F10ShowRun               | None                   | Returns the running configuration (in memory).                                 |
| F10ShowVer               | None                   | Returns software version information.                                          |
| F10ShowVlan              | None                   | Returns the <b>show vlan</b> output for all VLANs.                             |
| F10ShowVlanId            | (vlanId)               | Returns the <b>show vlan</b> output for a specific vlan.                       |
| F10ShowVlanIntStatus     | (vlanId)               | Returns the detailed status of a specified VLAN interface.                     |
| F10ShowVrrp              | None                   | Returns the full VRRP status output.                                           |
| F10ShowVrrpBrief         | None                   | Returns a brief VRRP session summary.                                          |
| F10Traceroute            | (ipAddress, timeout)   | Performs a traceroute operation to an IP address from the switch.              |
| F10WriteMem              | None                   | Write the running configuration to the startup configuration file.             |

## Running a Python API Script

When you run a Python script that invokes the API functions in [Table 7-4](#), logon credentials are read from the smartutils.cfg file, and a telnet session opens on the switch in which function calls are executed in the FTOS CLI. The script closes the telnet session after running all the CLI commands.

The `smartutils.cfg` file is the configuration file used by the Programmatic Interface package. It contains the user name and passwords required to log on to a switch via telnet and access the CLI to execute the function calls in a Python API script. The `smartutils.cfg` file downloads with the Programmatic Interface package and is stored at `/usr/pkg/scripts/smartutils`.



**Note:** Use the user name and passwords contained in the `smartutils.cfg` file to log into and run only the scripts created using the PERL, Python, and UNIX APIs described in this chapter. A username used to run scripts cannot contain special characters.

To configure the username and passwords located in the `smartutils.cfg` file that are used to run Python API scripts, do one of the following:

- From a UNIX shell, use the UNIX text editor to open the `smartutils.cfg` file, enter a user name and password, and save the file.

To run a Python API script:

- From the FTOS CLI, use the **script** command described in [Running Scripts with User Privileges](#).
- From a UNIX shell, follow the procedure described in [Running a Script from the UNIX Shell](#).

## Using UNIX Shell Scripting

To create a UNIX script using the UNIX API and run the script on a Dell Networking switch, use the information in this section. For information about creating and running a PERL or Python script using the PERL or Python API, see [Supported UNIX Utilities](#) and [Using the Python API](#).

### Creating a UNIX API Script

To create a UNIX shell script to be run on a Dell Networking switch, use the information in this section.

The `F10SmartScriptUtils.py` file is the main API library file that contains the functions that you can include in a UNIX shell script. The `F10SmartScriptUtils.py` file is stored at `/usr/pkg/scripts/smartutils`. [Table 7-5](#) describes the FTOS operations that you can invoke from a UNIX shell script, including the supported functions and required arguments.

[Figure 7-4](#) shows an example of how to write a script in the UNIX shell scripting language. You can store a UNIX shell script anywhere on the switch.

**Figure 7-4. Script Written in the UNIX Shell Scripting Language: Example**

```
#!/bin/sh

i=1
while [$i -le $2]
do
 echo $i
 /usr/pkg/bin/python /usr/pkg/scripts/smartutils/F10SmartScriptUtils.py createvlanid $i
 ((i++))
done
```

**Table 7-5. Supported API Functions in UNIX Shell Scripts**

| Function              | Arguments                               | Description                                                                             |
|-----------------------|-----------------------------------------|-----------------------------------------------------------------------------------------|
| addlaginttovlan       | lagId, vlanId, tagFlag                  | Adds a port channel (LAG) to a VLAN.<br>tagFlag values: 1 (tagged) or 0 (untagged).     |
| addphyinttovlan       | stackunitNum, portId<br>vlanId, tagFlag | Adds an interface to a VLAN.<br>tagFlag values: 1 (tagged) or 0 (untagged).             |
| createvlanid          | vlanId                                  | Creates a VLAN with a specified VLAN ID.                                                |
| deletevlanid          | vlanId                                  | Deletes a VLAN with a specified VLAN ID                                                 |
| makelagintnoshutdown  | lagId                                   | Enables the specified port channel.                                                     |
| makelagintshutdown    | lagId                                   | Disables the specified port channel.                                                    |
| makelagintswitch      | lagId                                   | Configures the specified port channel (LAG) as a Layer 2 switchport.                    |
| makephyintnoshutdown  | stackUnitNum, portId                    | Enables the specified port.                                                             |
| makephyintshutdown    | stackUnitNum, portId                    | Disables the specified port.                                                            |
| makephyintswitch      | stackunitNum, portId                    | Configures the specified port as a Layer 2 switchport.                                  |
| makevlanintnoshutdown | vlanId                                  | Enables the specified VLAN interface.                                                   |
| makevlanintshutdown   | vlanId                                  | Disables the specified VLAN interface.                                                  |
| ping                  | ipAddress                               | Pings (via ICMP) an IP address from the switch.                                         |
| showarptbl            | None                                    | Returns the table of learned ARP addresses.                                             |
| showbgpneighbors      | None                                    | Returns detailed BGP neighbor information.                                              |
| showbgproute          | None                                    | Returns BGP-learned routes.                                                             |
| showbgpsummary        | None                                    | Returns BGP peer summary and status.                                                    |
| showbootvar           | None                                    | Returns system boot variables.                                                          |
| showcmd               | command                                 | Executes a specified <b>show</b> command.                                               |
| showenvironment       | None                                    | Returns environment-monitoring variable values.                                         |
| showipintbrief        | None                                    | Returns full interface list with up/down status.                                        |
| showipintbriefflag    | None                                    | Returns brief interface status (up/down/ admin up/down) of all port-channel interfaces. |
| showipintbriefman     | None                                    | Returns brief interface status (up/down/ admin up/down) of all management interfaces.   |

**Table 7-5. Supported API Functions in UNIX Shell Scripts (continued)**

|                       |                      |                                                                                     |
|-----------------------|----------------------|-------------------------------------------------------------------------------------|
| showipintbriefphy     | None                 | Returns brief interface status (up/down/ admin up/down) of all physical interfaces. |
| showipintbriefvlan    | None                 | Returns brief interface status (up/down/ admin up/down) of all VLAN interfaces.     |
| showiproute           | None                 | Returns switch routing table.                                                       |
| showisisneighbors     | None                 | Returns detailed ISIS neighbor information.                                         |
| showisisroute         | None                 | Returns ISIS-learned routes.                                                        |
| showlagintstatus      | lagId                | Returns detailed status information for a specified port channel.                   |
| showlagintvlanmembers | lagId                | Returns VLAN membership of a specified port channel.                                |
| showlog               | None                 | Returns system log output.                                                          |
| showmacaddrtbl        | None                 | Returns the table of learned MAC addresses.                                         |
| showmem               | lagId                | Returns switch memory usage.                                                        |
| showospfneighbors     | None                 | Returns detailed OSPF neighbor information.                                         |
| showospfroute         | None                 | Returns OSPF-learned routes.                                                        |
| showphyintband        | stackunitNum, portId | Returns in/out bandwidth average for a specified port.                              |
| showphyintstatus      | stackunitNum, portId | Returns detailed status information for a specified port                            |
| showphyintvlanmembers | stackunitNum, portId | Returns VLAN membership of a specified port.                                        |
| showproccpu           | None                 | Returns switch CPU usage and running processes.                                     |
| showrun               | None                 | Returns the running configuration (in memory).                                      |
| showver               | None                 | Returns software version information.                                               |
| showvlan              | None                 | Returns information on all VLANs, including membership.                             |
| showvlanid            | vlanId               | Returns detailed interface information for a specified VLAN.                        |
| showvlanintstatus     | vlanId               | Returns VLAN interface status.                                                      |
| showvrrp              | None                 | Returns the full VRRP status output.                                                |
| showvrrpbrief         | None                 | Returns a brief VRRP session summary.                                               |
| traceroute            | ipAddress, timeout   | Performs a traceroute operation to an IP address from the switch.                   |
| writemem              | None                 | Write the running configuration to the startup configuration file.                  |

## Running a UNIX API Script

When you run a UNIX shell script that invokes the API functions in [Table 7-5](#), logon credentials are read from the smartutils.cfg file, and a telnet session opens on the switch in which function calls are executed in the FTOS CLI. The script closes the telnet session after running all the CLI commands.

The `smartutils.cfg` file is the configuration file used by the Programmatic Interface package. It contains the user name and passwords required to log on to a switch via telnet and access the CLI to execute the function calls in a UNIX API script. The `smartutils.cfg` file downloads with the Programmatic Interface package and is stored at `/usr/pkg/scripts/smartutils`.



**Note:** Use the user name and passwords contained in the `smartutils.cfg` file to log into and run only the scripts created using the PERL, Python, and UNIX APIs described in this chapter. A username used to run scripts cannot contain special characters.

To configure the username and passwords located in the `smartutils.cfg` file that are used to run UNIX API scripts, do one of the following:

- From a UNIX shell, use the UNIX text editor to open the `smartutils.cfg` file, enter a user name and password, and save the file.

To run a UNIX API script:

- From the FTOS CLI, use the **script** command described in [Running Scripts with User Privileges](#).
- From a UNIX shell, follow the procedure described in [Running a Script from the UNIX Shell](#).



# Virtual Server Networking

Virtual Server Networking is supported on platforms: **S60** **S55** **S4810**

As a part of the Open Automation package, Virtual Switch Networking (VSN) provides real-time communication between the Dell Networking network fabric and virtual servers to automate network management and configuration tasks throughout the data center. VSN provides a closed-loop provisioning system to enable, for example, the automatic re-provisioning of VLANs and port profiles across multiple switches simultaneously, thereby increasing employee productivity and minimizing human error.

Because Open Automation supports hypervisors from multiple vendors, data center managers can use a single mechanism to simultaneously support multiple hypervisors and their current management tools.

VSN is installed as a self-contained package, and requires the [Smart Scripting](#) package.



**Note:** VSN is not supported in stacked configurations; it is supported only on standalone switches.

This chapter includes the following:

- [Hypervisor Modes](#)
- [VLAN configuration](#)
- [Installing VSN](#)
- [Enabling VSN in a Hypervisor Session](#)
- [Running VSN Scripts](#)
- [Stopping a Hypervisor Session](#)
- [Uninstalling VSN](#)
- [Viewing VSN information](#)

## Overview

Virtual Server Networking is an Open Automation tool that enables Dell Networking switch/routers in a data center network to retrieve configuration information from hypervisors. VMware vSphere and Citrix Xen hypervisors are supported.

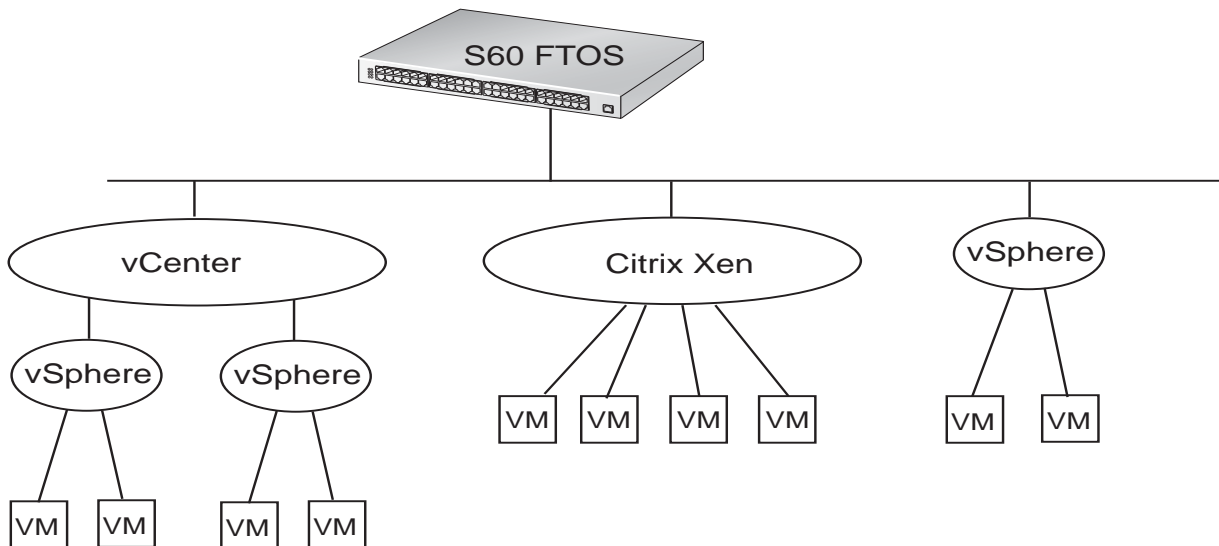
Both VMware and Citrix Xen provide SDKs and APIs for accessing their configuration objects. VSN requires Layer 3 connectivity to access a hypervisor.

Figure 8-1 shows an example of the network architecture in which a Dell Networking FTOS switch is connected to multiple servers, each of which may run a different type of hypervisor. The vCenter hypervisor from VMware is a centralized server management system that can manage multiple vSphere operating systems on which multiple virtual machines (VMs) can run. The VMware ESX server is a single unit, that may be managed by the hypervisor or act as an independent unit. The Citrix Xen hypervisor uses a distributed management methodology under which a number of XenServers are grouped in a management domain, with a master server managing the other units in the domain.

Minimal packet drops may be seen when migrating VMS from one server to another. The drops may vary from one second or higher, depending on the load on the server and network.

FTOS supports up to eight hypervisor sessions. A hypervisor session can consist of a single hypervisor unit (ESX, ESXi, XenServer) or a centralized hypervisor (vCenter, Xenpool). A vSphere client is used to manage a single VMware hypervisor. A vCenter server is a centralized management server for managing multiple VMware hypervisors.

**Figure 8-1. Virtual Server Networking example**



VSN subscribes to hypervisor for any change to be notified to switch. Depending on the hypervisor mode configured, FTOS may automatically update its configuration, provide provisioning for configuration changes, or require system administrator intervention.

## Hypervisor Modes

There are two modes for retrieving configuration information from a hypervisor on a virtual server:

- **Check:** VSN retrieves configuration information from a hypervisor and notifies the system administrator when there is a change in the network configuration; for example, when a VLAN is added or removed. A system administrator must make manual updates to the FTOS configuration.
- **Config:** VSN retrieves configuration information from a hypervisor and automatically makes the required configuration changes in FTOS on the switch.

## VSN Persistency

VSN installation and configuration is persistent in the FTOS configuration and remains after a system reload. However, the configuration information retrieved through a hypervisor is not persistent. If the system reloads, when it boots up the VSN application will retrieve the network configuration of virtual servers again and reconfigure FTOS accordingly.

## VLAN configuration

### Management VLAN

The management interface between a switch and a hypervisor can be a single port or VLAN interface. If the connection with a hypervisor is through a VLAN, you must manually configure the VLAN interface on the switch before VSN can establish a connection with the hypervisor and retrieve information from it about virtual-server configuration.

A hypervisor's management interface can also be a data interface, which means both management traffic and data traffic can use the same interface.

Manually configured VLANs are not removed by VSN after application or configuration changes are made in FTOS on a switch.

## Data VLANs

Hypervisor-aware VLANs used for data traffic are automatically configured according to the configuration parameters retrieved from the hypervisor by VSN as part of the VLAN trunk on the switch port.

Enter the **show vlan** command to display the VSN hypervisor-learned VLANs on the switch. As shown in [Figure 8-2](#), VSN VLANs that have been automatically configured are displayed with a **G** tag in the left-most column and are associated with ports marked with an **H** tag. If a VSN VLAN has been manually configured on the switch, the VLAN has no tag; the associated ports are displayed with an **H** tag.

**Figure 8-2. Display VSN Hypervisor-learned VLANs: show vlan**

```
FTOS(conf-hypervisor)#show config
!
Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs,
 P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
 x - Dot1x untagged, X - Dot1x tagged
 G - GVRP tagged, M - Vlan-stack, H - VSN tagged
 i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT
 tagged

 NUM Status Description Q Ports
* 1 Active U Te 0/0,15,25,27,29,42-43
 U Te 11/35-36
G 4001 Active H Te 0/35
G 4002 Active H Te 0/35
 4003 Active H Te 0/35
 T Te 0/15
```

## Hypervisor-unaware VLANs

VSN cannot discover VLAN configurations from a hypervisor. If an application requires a hypervisor-unaware VLAN, you must configure the VLAN manually. User-configured VLANs are not removed when VSN retrieves and updates a network configuration.

## Installing VSN

VSN is installed as a separate Open Automation package, apart from the FTOS image and the downloaded Smart Scripting package. When you install the VSN package, VSN is loaded into FTOS.



**Note:** VSN is not supported in stacked configurations; it is only supported on standalone switches.

You install the VSN package file in the same way as you install an FTOS release: directly from local flash memory on a switch or from an external drive on a network server. Because the installation takes time, it is performed in the background. When the download is complete, a message is displayed on the console. The package installation updates the running-configuration file.

You must manually configure the interfaces used to connect to hypervisors. Refer to the *FTOS Configuration Guide, Interfaces* chapter for information on how to configure a VLAN or physical interface.

**Prerequisites:**

- Smart Scripting is a prerequisite for using Virtual Server Networking. You must first install the Smart Scripting package before you can run the VSN application (see [Installing Smart Scripting](#))

To install the VSN package:

1. On a PC or other network device, go to the Dell Networking web portal at <https://www.force10networks.com/CSPortal20/Main/SupportMain.aspx>. Click **Login**, enter your user ID and password, and click the **Login** button.
2. On the Customer Support page, click the **Software Center** tab.
3. In the left-hand column, click **Automation Software**.
4. At the bottom of the Terms and Conditions page, click **I agree**.
5. On the Automation Software page, under Software, click the **VSNAGENT2.0.x.tar.gz** file.
6. In the dialog box, select the path for the local flash on the switch or a directory path on a network server where you want to download the VSNAGENT2.0.x.tar.gz file.
7. When the download is complete, enter the **package install** command from the FTOS CLI on a switch to install the VSN package in the internal flash memory.

| Command Syntax                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Command Mode   | Task                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------|
| <b>package install {flash://filename   ftp://userid:password@host-ipaddress/dir-path   tftp://host-ipaddress/dir-path}</b><br>Where: <ul style="list-style-type: none"> <li>• <b>flash://filename</b> installs the VSN file stored in flash memory on the switch.</li> <li>• <b>ftp://userid:password@host-ipaddress/filepath</b> logs in and installs VSN from a file stored on an FTP server.</li> <li>• <b>tftp://host-ipaddress/filepath</b> installs VSN from a file stored on a TFTP server.</li> </ul> | EXEC Privilege | Install the VSN package in the running configuration of the switch from local flash memory or a network server. |

8. Enter the following command to configure the Perl script (VSNAgent.pl) used for VSN operations on VMware hypervisors: `script /usr/pkg/scripts/VSNAgent/VMWare/VSNAgent.pl`.

To follow the progress of a package installation (or removal), enter the **show packages** command.

## Enabling VSN in a Hypervisor Session

### Restrictions:

- VSN is not supported in stacked configurations; it is only supported on standalone units.
- VSN supports connections only with VMware and Xen hypervisors
- You can define up to eight hypervisor sessions on a switch.
- To connect with a VMware hypervisor running on an ESXi 5.0 server, you must configure the server's firewall to allow connections only through the management IP address. You can reconfigure the firewall by using the **esxcli network firewall** command to create a rule set that allows the IP address of a Dell Networking switch to pass the firewall. For detailed information, refer to *How to Create Custom Firewall Rules in ESXi 5.0*.
- When you establish a VSN session with a Citrix Xen hypervisor (**access** command) that operates as a slave in a pool, the connection is established with the master. Configuration and access information is retrieved from the entire pool. If the slave is removed from the pool and operates as a standalone hypervisor, the VSN session is still active with the master. In this case, information is retrieved from the pool and not from the standalone hypervisor.

To enable VSN on an interface and connect to hypervisors on network servers:

| Step | Task                                                                                                                                                           | Command Syntax                                                                        | Command Mode  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------|
| 1    | Enable VSN on an interface.                                                                                                                                    | <b>vsn enable</b><br>VSN is disabled by default on switch interfaces.                 | INTERFACE     |
| 2    | Specify the name of a hypervisor session and enter hypervisor configuration mode.                                                                              | <b>hypervisor name</b><br>Enter up to 40 characters to define the hypervisor session. | CONFIGURATION |
| 3    | Define the hypervisor type to which you want to connect. Use the <b>show hypervisor supported</b> command to display the currently supported hypervisor types. | <b>type {vmware   xen-citrix}</b><br>There is no default value.                       | HYPERVISOR    |

| Step | Task                                                                                                | Command Syntax                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Command Mode |
|------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| 4    | Establish the connection between the switch and a hypervisor                                        | <p><b>access</b> <i>url</i> <b>username</b> <i>username</i><br/> <b>password</b> <i>password</i></p> <p>Where <i>url</i> is one of the following values:<br/> For a VMware hypervisor:<br/> <b>https://[ip-address]/sdk/vimService</b><br/> <b>username</b> [<i>name</i>] <b>password</b> [<i>password</i>]</p> <p>For an Xen hypervisor:<br/> <b>http://ip-address</b> <b>username</b> [<i>name</i>]<br/> <b>password</b> [<i>password</i>]</p> <p><b>username</b> <i>name</i>: Username to be used for authentication on the server.<br/> <b>password</b> <i>password</i>: Password to be used for authentication shown in clear text.</p> | HYPERVERISOR |
| 5    | Set the mode for retrieving virtual server configurations and updating FTOS settings on the switch. | <p><b>mode</b> { <b>check</b>   <b>config</b> }</p> <p><b>check</b>: Retrieve configuration information from the hypervisor, and notify the system administrator of any configuration changes. The configuration changes need to be entered manually on the switch.</p> <p><b>config</b>: Retrieve configuration information and automatically update the configuration parameters in FTOS on the switch.</p> <p>Default: <b>config</b>.</p>                                                                                                                                                                                                 | HYPERVERISOR |
| 6    | Enable the defined hypervisor connection.                                                           | <b>no disable</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | HYPERVERISOR |

After you enable VSN on an interface and enable a hypervisor session that connects to hypervisors on network servers, you can change the **mode** setting when the session is active. You cannot, however, change the **type** and **access** settings if the session is active. To change these settings, you must:

1. In hypervisor configuration mode, stop the session by entering the **disable** command.
2. Enter the **no type** { **vmware** | **xen-citrix** } or **no access** *url* **username** *username* **password** *password* command to remove a configured setting.
3. Enter the **type** { **vmware** | **xen-citrix** } or **access** *url* **username** *username* **password** *password* command to configure a new setting.

## Discovery

The discovery process starts after you enter the **no disable** command on the interface and ends 10 minutes after connectivity is established between the switch and hypervisor. If no connectivity is established, the switch attempts to connect for three minutes and then stops. Refer to [Connectivity](#) for more details on this process.

After you enable the link between a switch and a hypervisor, the switch uses a discovery mechanism to learn VMAC and VLAN information from the hypervisor. The discovery process also starts in the following conditions:

- You enter the **shutdown** and **no shutdown** commands on a VSN-enabled port. The discovery process resumes on the individual port only, not on all enabled ports.
- You enter the **disable** and **no disable** commands in hypervisor configuration mode for a specified type of hypervisor connection. The discovery process is resumed on all enabled ports.
- An update arrives from a hypervisor. The discovery process resumes on all VSN-enabled ports.

In order for a switch to learn VLAN information from a hypervisor:

- Incoming traffic must be received on the VSN-enabled ports.
- There must be at least one VMAC configured on the hypervisor so that the VCAP table can capture the VMAC entries for each VSN-enabled port.

The following log messages are displayed when the discovery process is interrupted and when it starts again.

### Message 1

```
Nov 28 11:34:19: %STKUNIT0-M:CP %VSNMGR-5-VSN_DISCOVERY_SUSPENDED:
Hypervisor macs not seen on Te 0/25. Discovery suspended.
```

### Message 2

```
Nov 28 11:40:36: %STKUNIT0-M:CP %VSNMGR-5-VSN_DISCOVERY_RESUMED: Detected
config change in Hypervisor. Discovery of Hypervisor macs resumed on Te 0/25.
```

## Connectivity

If a network server is not reachable, a log message is displayed and the VSN agent tries periodically to establish the connection with the hypervisor. The initial log message is:

### Message 3

```
Xen-Citrix:Connection error for hypervisor testing:LOGIN FAILURE
```



If connectivity to a hypervisor is lost after information is retrieved and used to reconfigure a switch, the following log message is displayed. The VSN agent tries to connect to the hypervisor in the background. The information that was retrieved from the hypervisor is not deleted.

#### Message 4

```
Xen-Citrix:Lost connection to hypervisor xen217. Retrying...
```

Afterwards, one of the following actions is performed:

- If connectivity with the hypervisor is re-established within three minutes after the loss of connectivity, the following log message is displayed and the retrieved information is retained:

#### Message 5

```
Xen-Citrix:Reestablished connection with hypervisor xen217.
```

- If connectivity with the hypervisor is not re-established within three minutes after the loss of connectivity, the following log message is displayed. The information retrieved from the hypervisor is deleted and the VLANs from the hypervisor are unconfigured:

#### Message 6

```
Xen-Citrix:Lost connection to hypervisor xen217. Removing learnt information.
```

## Running VSN Scripts

The VSN package contains the SDKs for VMware and Citrix Xen hypervisors. The Perl and Python scripts required for VSN functionality are stored with the VSN 2.0.x package in the **/usr/pkg/scripts/VSNAgent** directory as follows:

- For VMware hypervisors, the Perl script is stored is at **/usr/pkg/scripts/VSNAgent/VMWare/VSNAgent.pl**.
- For Citrix Xen hypervisors, the Python script is stored is at **/usr/pkg/scripts/VSNAgent/Xen/hpAgtMain.py**



**Caution:** The Dell Open Automation Virtual Server Networking™ software package (the “Product”) may contain the VMware SDK for Perl, which is licensed by VMware, Inc. VMware will not provide technical support for the VMware SDK included in the Product. Users interested in writing scripts for VMware products must obtain the VMware SDK directly from VMware. You may not create scripts for VMware products through use of the VMware SDK included in the Virtual Server Networking package. End Users may use the Dell Virtual Server Networking according to the terms, conditions, and limitation of the pertinent Dell End User License Agreement only.

To run a VSN script (Perl or Python) in all connected hypervisor sessions to retrieve virtual server configurations and update FTOS settings on the switch, enter the **script** command in configuration mode.

| Command Syntax                   | Command Mode  | Task                                                                                                                                                                                                                                                               |
|----------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>script</b> <i>script-name</i> | CONFIGURATION | Run a VSN script in active sessions on VMware and Xen hypervisors.<br>For <i>script-name</i> , enter the directory path and filename where the VSN script is stored on the switch; for example: <code>script /usr/pkg/scripts/VSNAgent/VMWare/VSNAgent.pl</code> . |



**Note:** The **script** command is not supported on S55 switches to run VSN scripts.

To stop a VSN script that is running, enter the **no** version of the **script** *script-name* command; for example: **no script /usr/pkg/scripts/VSNAgent/VMWare/VSNAgent.pl**.

## Stopping a Hypervisor Session

### Disabling a Session

Enter the **disable** command in HYPERVERSOR mode to stop VSN in a hypervisor session. The **disable** command does not remove connectivity with the hypervisor or remove the session information from the system configuration.

| Command Syntax | Command Mode | Task                                   |
|----------------|--------------|----------------------------------------|
| <b>disable</b> | HYPERVERSOR  | Shut down VSN in a hypervisor session. |

### Removing a Session

Use the **no hypervisor** command in CONFIGURATION mode to delete the configuration of a hypervisor session from the running configuration. The **no hypervisor** command deletes the specified configuration and closes an active hypervisor session, but does not remove the VSN agent from your system.

| Command Syntax                   | Command Mode  | Task                                                                                                   |
|----------------------------------|---------------|--------------------------------------------------------------------------------------------------------|
| <b>no hypervisor</b> <i>name</i> | CONFIGURATION | Delete a session from the system.<br>Enter the name of the hypervisor session that you want to remove. |

# Uninstalling VSN



**Caution:** Before you uninstall the VSN package, you must first stop all VSN scripts that are currently running using the **no script** *script-name* command.

Uninstalling the VSN package removes it from the internal flash memory on a switch.

| Command Syntax                                                                                                                   | Command Mode   | Task                                       |
|----------------------------------------------------------------------------------------------------------------------------------|----------------|--------------------------------------------|
| <b>package uninstall</b> <i>name</i><br>Enter the name of the VSN package, exactly as it appears in <b>show packages</b> output. | EXEC Privilege | Uninstall the VSN package from the system. |

## Viewing VSN information

To view the configuration of currently active hypervisor sessions, enter the **show configuration** command in HYPERVISOR mode.

| Command Syntax            | Command Mode | Task                                                  |
|---------------------------|--------------|-------------------------------------------------------|
| <b>show configuration</b> | HYPERVISOR   | Display configuration of current hypervisor sessions. |

**Figure 8-3. Display a Hypervisor Session: show configuration**

```
FTOS(conf-hypervisor)#show config
!
hypervisor LocalNetwork
mode config
access https://10.10.10.10 username admin password 7 1d28e9f33f99cf5c
```

To display a list of currently supported hypervisors, enter the **show hypervisors supported** command.

| Command Syntax                   | Command Mode   | Task                                     |
|----------------------------------|----------------|------------------------------------------|
| <b>show hypervisor supported</b> | EXEC Privilege | Display a list of supported hypervisors. |

**Figure 8-4. Display Supported Hypervisors: show hypervisor supported**

```
FTOS#show hypervisor supported
vmware
xen-citrix
```

To display the components of current hypervisor sessions, including the link, virtual switch, and hypervisor to which the switch is connected, enter the **show virtualswitch** command.

| Command Syntax                                                                  | Command Mode   | Task                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show virtualswitch</b> [ <i>interface</i> ]<br>[ <i>virtualswitch-name</i> ] | EXEC Privilege | Display general information on current hypervisor sessions. To display detailed information on a hypervisor session, enter the VSN interface and/or virtual-switch name generated by the hypervisor as displayed in <b>show virtualswitch</b> output (Figure 8-6). |

**Figure 8-5. Display All Hypervisor Sessions: show virtualswitch**

```
FTOS#show virtualswitch
Interface VSwitch Hypervisor
Gi 0/32 vSwitch3 VMWare_vmware207
Po 7 vSwitch1 VMWare_vmware206
```

**Figure 8-6. Display a Specified Hypervisor Sessions: show virtualswitch**

```
FTOS#show virtualswitch GigabitEthernet 0/32 vSwitch3
Interface :Gi 0/32
Hypervisor Type :vmware
Hypervisor Name :vmware207
Hypervisor Version :4.1.0
Virtual Switch :vSwitch3
Port groups :
 Name :VLAN 3
 Vlan Id :138
 VIFs:
 MAC MTU
 00:50:56:92:00:77 8000
 Name :VM Network 4
 Vlan Id :-
 VIFs:
 MAC MTU
 00:0c:29:4f:66:19 8000
PIFs:
 MAC MTU
 00:26:55:dd:01:4f 8000
```

To display information on the virtual machines accessed on a switch interface, including the virtual machine name, VMAC address, and corresponding VLAN ID, enter the **show vmmmap** command.

| Command Syntax                      | Command Mode   | Task                                                         |
|-------------------------------------|----------------|--------------------------------------------------------------|
| <b>show vmmmap</b> <i>interface</i> | EXEC Privilege | Display the virtual machines accessed on a switch interface. |

**Figure 8-7. Display Virtual Machines Accessed on an Interface: show vmmmap**

```
FTOS#show vmmmap gigabitethernet 0/32
VM Name VIF Vlan ID
Redhat_207_03_nfs 00:0c:29:4f:66:19 -
Redhat_207_03_nfs 00:50:56:92:00:77 138
```



**Note:** In **show vmmmap** and **show virtualswitch** output, VLAN 1 is displayed as VLAN ID 1; VLAN 4095 is displayed without a VLAN ID as "- "



# Virtual Server Networking CLI

## Overview

Virtual Server Networking CLI is supported on platforms: **S60** **S55** **S4810**



**Note:** VSN is not supported in stacked configurations; it is only supported on standalone switches.

## Commands

- access
- disable
- hypervisor
- mode
- package install
- package uninstall
- script
- show hypervisor supported
- show packages
- show virtualswitch
- show vmmmap
- type
- vsn enable

## access

S55 S60 S4810

Configure the connection to access a hypervisor.

### Syntax

**[no] access** *url username name password password*

### Parameters

|                                 |                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>url</i>                      | Enter the URL location of the desired hypervisor.<br>For a VMware hypervisor, enter:<br><b>https://[ip-address]/sdk/vimService username [name] password [password]</b><br>For a Xen hypervisor, enter:<br><b>http://ip-address username [name] password [password]</b> |
| <b>username</b> <i>name</i>     | Enter the user name to be used for authentication.                                                                                                                                                                                                                     |
| <b>password</b> <i>password</i> | Enter the password to be used for authentication in clear text.                                                                                                                                                                                                        |

### Defaults

None

### Command Modes

HYPERVISOR

### Command History

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |

### Usage Information

VSN tries to establish a connection with a hypervisor only after the user credentials (user name and password) are configured with the **access** command.

## disable

S55 S60 S4810

Stop a hypervisor session.

### Syntax

**[no] disable**

### Defaults

disable

### Command Modes

HYPERVISOR

### Command History

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |

### Usage Information

Entering the **disable** command in hypervisor configuration mode disables VSN in the current hypervisor session. It does not remove connectivity with the hypervisor or remove the session information from the system configuration.

Enter **no disable** to re-enable a configured hypervisor session.



# hypervisor

S55 S60 S4810

Specify the name of a hypervisor session with which VSN will connect.

**Syntax** **[no] hypervisor name**

|                   |             |                                                                                                                        |
|-------------------|-------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>name</i> | Enter up to 40 characters to specify the name of a hypervisor session to which you want to connect on network servers. |
|-------------------|-------------|------------------------------------------------------------------------------------------------------------------------|

**Defaults** None

**Command Modes** CONFIGURATION

|                        |                 |                          |
|------------------------|-----------------|--------------------------|
| <b>Command History</b> | Version 8.3.8.0 | Introduced on the S4810. |
|                        | Version 8.3.5.1 | Introduced on the S55.   |
|                        | Version 8.3.3.4 | Introduced on the S60.   |

**Usage Information** After you enter the command, you are placed in hypervisor configuration mode to configure settings for the session.

Enter the **no hypervisor name** command to remove the configuration of a specified hypervisor session from the running configuration and close active hypervisor sessions without removing the VSN agent from the system.

# mode

S55 S60 S4810

Set the hypervisor mode used to retrieve configuration information on virtual servers.

**Syntax** **[no] mode { check | config }**

**Defaults** **config**

|                   |               |                                                                                                                                                                                                                                                                                          |
|-------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <b>check</b>  | VSN retrieves configuration information about virtual servers from a hypervisor and notifies the system administrator if the configuration has changed (for example, a VLAN has been added or removed). Changes in FTOS configuration parameters must be entered manually on the switch. |
|                   | <b>config</b> | VSN retrieves configuration information from the Hypervisor and implements any necessary configuration changes automatically.                                                                                                                                                            |

**Command Modes** HYPERVISOR

|                        |                 |                          |
|------------------------|-----------------|--------------------------|
| <b>Command History</b> | Version 8.3.8.0 | Introduced on the S4810. |
|                        | Version 8.3.5.1 | Introduced on the S55.   |
|                        | Version 8.3.3.4 | Introduced on the S60.   |

**Usage Information**

You can use the **mode** command to change the way in which virtual-server information is retrieved in an existing hypervisor session.

The following log messages are displayed when the hypervisor mode **check** is used to retrieve configuration information on virtual servers:

**Message 1**

```
Dec 1 04:57:48: %STKUNIT0-M:CP %VSNMGR-5-VSN_VLAN_DISCOVERY: Te 0/35, Vlan: 4001-4008, 4011-4012
```

**Message 2**

```
Dec 1 04:56:46: %STKUNIT0-M:CP %VSNMGR-5-VSN_VLAN_WITHDRAWAL: Te 0/35, Vlan: 4001-4008, 4011-4012
```

## package install

S55 S60 S4810

Install an Open Automation package, such as Virtual Server Networking. This command downloads the package from the specified location, and installs it in the internal flash memory on a switch.

**Syntax**

**package install** *location*

**Parameters**

*location*

Enter the location where you want to install an Open Automation package, where *location* is one of the following values:

- **flash://filename** installs the VSN package file stored in flash memory on the switch.
- **ftp://userid:password@host-ip-address/file-path** logs in and installs VSN from a file stored on an FTP server.
- **tftp://host-ip-address/file-path** installs VSN from a file stored on a TFTP server.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

Version 8.3.8.0 Introduced on the S4810.

Version 8.3.5.1 Introduced on the S55.

Version 8.3.3.4 Introduced on the S60.

**Usage Information**

Because the installation of the VSN package takes time, the installation is performed in the background. When the download is complete, a message is displayed on the console.

To follow the progress of a package installation, enter the [show packages](#) command.

# package uninstall

S55 S60 S4810

Remove an installed Open Automation package, such as Virtual Server Networking, from the system.

**Syntax** `package uninstall name`

|                   |             |                                                                                                                 |
|-------------------|-------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>name</i> | Enter the name of the Open Automation package, exactly as it appears in the <a href="#">show packages</a> list. |
|-------------------|-------------|-----------------------------------------------------------------------------------------------------------------|

**Defaults** None

**Command Modes** EXEC Privilege

|                        |                 |                          |
|------------------------|-----------------|--------------------------|
| <b>Command History</b> | Version 8.3.8.0 | Introduced on the S4810. |
|                        | Version 8.3.5.1 | Introduced on the S55.   |
|                        | Version 8.3.3.4 | Introduced on the S60.   |

**Usage Information** Uninstalling the VSN package removes it from the internal flash memory on the switch. To follow the progress when removing a package from the system, enter the [show packages](#) command.



**Caution:** Before you uninstall the Virtual Server Networking package, you must first stop all scripts that are currently running using the **no script script-name** command.

|                         |                               |                                                   |
|-------------------------|-------------------------------|---------------------------------------------------|
| <b>Related commands</b> | <a href="#">show packages</a> | Display all the packages installed in the system. |
|-------------------------|-------------------------------|---------------------------------------------------|

# script

S60 S4810

Run an installed VSN script (Perl or Python) on active hypervisor links to retrieve virtual server configurations and update FTOS settings on the switch.

**Syntax** `[no] script script-name`

Enter the **no script script-name** to stop a running script.

|                   |                    |                                                                                                                                     |
|-------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b> | <i>script-name</i> | Enter the directory path and filename of where the VSN script is stored; for example, /usr/pkg/scripts/VSNAgent/VMWare/VSNAgent.pl. |
|-------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|

**Defaults** None

**Command Modes** CONFIGURATION

|                        |                 |                          |
|------------------------|-----------------|--------------------------|
| <b>Command History</b> | Version 8.3.8.0 | Introduced on the S4810. |
|                        | Version 8.3.3.4 | Introduced on the S60.   |

**Usage Information**

For VMware hypervisors, the VSNAgent.pl Perl script is stored in the /usr/pkg/scripts/VSNAgent/VMWare directory.

For Xen Citrix hypervisors, the hpAgtMain.py Python script is stored in the /usr/pkg/scripts/VSNAgent/Xen directory.



**Note:** The **script** command used to run VSN scripts is not supported on S55 switches.

## show hypervisor supported

S55 S60 S4810

Display the types of hypervisors currently supported by VSN.

**Syntax**

**show hypervisor supported**

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |

**Usage Information**

Use this information when defining types of hypervisor connections with the [hypervisor](#) command.

**Related Commands**

|                            |                               |
|----------------------------|-------------------------------|
| <a href="#">hypervisor</a> | Define a hypervisor instance. |
|----------------------------|-------------------------------|

**Example**

```
FTOS#show hypervisor supported
vmware
xen-citrix
```

## show packages

S55 S60 S4810

Display all Open Automation packages installed on a switch.

**Syntax**

**show packages**

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |

**Example**

```
FTOS#show packages

* Package Name:SMARTSCRIPTS Version: 2.0.0

 Python 2.6.5

 Perl 5.8.8
 Data::Dumper 2.126
 Class::MethodMaker 2.16
 ExtUtils::MakeMaker 6.56
 XML::NamespaceSupport 1.11
 XML::SAX 0.96
 XML::LibXML 1.70
 Compress::Raw::Bzip2 2.027
 Compress::Raw::Zlib 2.027
 IO::Compress 2.027
 URI 1.54
 HTML::Tagset 3.20
 HTML::Parser 3.65
 LWP 5.836
 Net::Telnet 3.03
 OSSP::uuid 1.0602
 UUID 0.02
 version 0.82
 Class::Inspector 1.24
 Task::Weaken 1.03
 Algorithm::Diff 1.1902
 Text::Diff 1.37
 SOAP::Lite 0.712
 Crypt::SSLeay 0.57
 URI::urn::uuid 0.03
 UUID 0.03
 Crypt::SSLeay 0.57
 Net::SNMP 6.0.0
 Net::Telnet::Cisco 1.10

 HTTP Server
 mini_httpd 1.19

 Perl and Python function library for Force10 SmartScripts
 smartutils 2.0.0

 WebConnect Web UI and CGI scripts
 htdocs 2.0.0

* Package Name:VSNAGENT Version: 2.0.0

 Python 2.6.5
 XenAPI

 Perl 5.8.8
 VIPerlToolkit 4.1

 VSNAgent Scripts

```

# show virtualswitch

S55 S60 S4810

Display the components of current hypervisor sessions, including the virtual switch and name of the hypervisor session to which a switch interface is connected,

**Syntax** `show virtualswitch [interface] [virtualswitch-name]`

**Defaults** None

## Parameters

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interface</i>          | Display information on the hypervisor session established on a specified interface. Enter one of the following interface types: <ul style="list-style-type: none"> <li>For a 100/1000 Ethernet interface or 1-Gigabit Ethernet interface, enter: <b>GigabitEthernet</b> <i>slot/port</i></li> <li>For a 10-Gigabit Ethernet interface, enter: <b>TenGigabitEthernet</b> <i>slot/port</i></li> <li>For a port-channel interface, enter: <b>port-channel</b> <i>number</i><br/>Where the valid port-channel numbers are 1 to 128.</li> </ul> |
| <i>virtualswitch-name</i> | Display information on a specified virtual switch by entering the name generated by the hypervisor.                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Command Modes** EXEC Privilege

## Command History

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |

## Usage Information

Use the **show virtualswitch** command to display the interface, virtual-switch name, and hypervisor-session name for all current hypervisor connections on the switch.

To display detailed information on a hypervisor session, re-enter the command with the interface and virtual-switch name for the session from the **show virtualswitch** output as shown in the example below.

## Example

The following command output displays information on the hypervisor sessions established on all virtual switches on network servers connected to switch interfaces.

```
FTOS#show virtualswitch
Interface VSwitch Hypervisor
Gi 0/32 vSwitch3 VMWare_vmware207
Po 7 vSwitch1 VMWare_vmware206
```

The following command output displays information on the hypervisor session established on virtual switch vSwitch3 on a VMware server connected to the interface 0/32.

```

FTOS#show virtualswitch Gigabitethernet 0/32 vSwitch3
Interface :Gi 0/32
Hypervisor Type :vmware
Hypervisor Name :vmware207
Hypervisor Version :4.1.0
Virtual Switch :vSwitch3
Port groups :
 Name :VLAN 3
 Vlan Id :138
 VIFs:
 MAC : MTU
 00:50:56:92:00:77 : 8000
 Name :VM Network 4
 Vlan Id :-
 VIFs:
 MAC : MTU
 00:0c:29:4f:66:19 : 8000
PIFs:
 MAC : MTU
 00:26:55:dd:01:4f : 8000

```



**Note:** In `show virtualswitch` output, VLAN 1 is displayed as VLAN ID 1; VLAN 4095 is displayed without a VLAN ID as "- "

## show vmmmap

S55 S60 S4810

Display the virtual machines accessed on a switch interface.

### Syntax

`show vmmmap interface`

### Defaults

None

### Parameters

*interface*

Display information on the virtual machines accessed on a specified interface. Enter one of the following interface types:

- For a 100/1000 Ethernet interface or 1-Gigabit Ethernet interface, enter: **GigabitEthernet** *slot/port*
- For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** *slot/port*
- For a port-channel interface, enter: **port-channel** *number*  
Where the valid port-channel numbers are 1 to 128.

### Command Modes

EXEC Privilege

### Command History

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |

**Usage Information**

The `show vmmmap` command displays information on the virtual machines accessed on a switch interface, including the virtual machine name, VMAC address, and corresponding VLAN ID

**Related Commands**

|                            |                               |
|----------------------------|-------------------------------|
| <a href="#">hypervisor</a> | Define a hypervisor instance. |
|----------------------------|-------------------------------|

**Example**

```
FTOS#show vmmmap gigabitethernet 0/32
VM Name VIF Vlan ID
Redhat_207_03_nfs 00:0c:29:4f:66:19 -
Redhat_207_03_nfs 00:50:56:92:00:77 138
```



**Note:** In `show vmmmap` output, VLAN 1 is displayed as VLAN ID 1; VLAN 4095 is displayed without a VLAN ID as "- "

## type

**S55** **S60** **S4810**

Set the hypervisor type to which you want to connect.

**Syntax**

**[no] type { vmware | xen-citrix }**

**Defaults**

None

**Parameters**

|                   |                                        |
|-------------------|----------------------------------------|
| <b>vmware</b>     | Set the hypervisor type as VMware.     |
| <b>xen-citrix</b> | Set the hypervisor type as Xen-Citrix. |

**Command Modes**

HYPERVERISOR

**Usage Information**

You must configure a hypervisor type in order to enable VSN connections with virtual servers. Use the `show hypervisor supported` command to display the currently supported hypervisor types.

**Command History**

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
| Version 8.3.5.1 | Introduced on the S55.   |
| Version 8.3.3.4 | Introduced on the S60.   |



# vsn enable

S55 S60 S4810

Enable VSN on an interface.

## Syntax

**[no] vsn enable**

## Defaults

VSN is disabled by default on switch interfaces.

## Command Modes

INTERFACE

## Command History

---

|                 |                          |
|-----------------|--------------------------|
| Version 8.3.8.0 | Introduced on the S4810. |
|-----------------|--------------------------|

---

|                 |                        |
|-----------------|------------------------|
| Version 8.3.5.1 | Introduced on the S55. |
|-----------------|------------------------|

---

|                 |                        |
|-----------------|------------------------|
| Version 8.3.3.4 | Introduced on the S60. |
|-----------------|------------------------|

---

## Usage Information

Enter the **vsn enable** command only on hypervisor-facing interfaces. **DO NOT** enter this command on an interface used for inter-switch links.

Enter the **no vsn enable** command to remove the VSN configuration from the system. You must reconfigure VSN to re-enable a hypervisor session.



# Smart Scripting CLI

## Overview

Smart Scripting 3.0 is supported on **S4810** S4820T sZ9000, MXL Switch platforms.

## Commands

- `mount nfs`
- `package install`
- `package uninstall`
- `script (run)`
- `script (stop/resume/kill/unschedule)`
- `script execute (EXEC mode)`
- `script execute (CONFIGURATION mode)`
- `script execute triggered-by`
- `script get`
- `script list execute`
- `script path`
- `script remove`
- `script trigger-event`
- `show packages`
- `show script`
- `start shell`
- `username`

### mount nfs

**S4810** S4820T  
Z9000, MXL  
Switch

Configure the folders to be used through a network file system (NFS).

**Syntax**                    **mount nfs** *nfs-server-ip: remote\_dir mount\_name [username username password password]*

To return to the default values, use the **no mount** command.

|                         |                                                                             |                                                                                                                   |
|-------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b>       | <b>remote_dir</b>                                                           | Enter the directory path where the network file system will be mounted.                                           |
|                         | <b>mount_name</b>                                                           |                                                                                                                   |
|                         | <b>username</b> <i>username</i>                                             | (Optional) Enter the keyword <b>username</b> followed by a text string up to 40 characters long as the user name. |
|                         | <b>password</b> <i>password</i>                                             | (Optional) Enter the keyword <b>password</b> followed by a text string up to 40 characters long as the password.  |
| <b>Defaults</b>         | None                                                                        |                                                                                                                   |
| <b>Command Modes</b>    | CONFIGURATION                                                               |                                                                                                                   |
| <b>Command History</b>  | Version 9.2(0.0)    Introduced on the S4810, S4820T, Z9000, and MXL Switch. |                                                                                                                   |
| <b>Related commands</b> | <a href="#">script path</a>                                                 | Configure the search path for the script or the NFS-mounted directory path.                                       |

## package install

S55 S60

S4810 Z9000  
MXL Switch

Install the Smart Scripting package. This command downloads the package from the specified location and installs it in the internal flash memory on a switch.

**Syntax**                    **package install** *location*

|                        |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b>      | <i>location</i>                                   | Enter the location from where you will download and install an Open Automation package, where <i>location</i> is one of the following values: <ul style="list-style-type: none"> <li>From the local flash: <b>flash://filename</b></li> <li>From an FTP server: <b>ftp://userid:password@host-ipaddress/filepath</b></li> <li>From a TFTP server: <b>tftp://host-ipaddress/filepath</b></li> </ul> |
|                        |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Defaults</b>        | None                                              |                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Command Modes</b>   | EXEC Privilege                                    |                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Command History</b> | Version 9.2(0.0)    Introduced on the MXL switch. |                                                                                                                                                                                                                                                                                                                                                                                                    |
|                        | Version 9.0.0.0    Introduced on the Z9000.       |                                                                                                                                                                                                                                                                                                                                                                                                    |
|                        | Version 8.3.8.0    Introduced on the S4810.       |                                                                                                                                                                                                                                                                                                                                                                                                    |
|                        | Version 8.3.5.1    Introduced on the S55.         |                                                                                                                                                                                                                                                                                                                                                                                                    |
|                        | Version 8.3.3.4    Introduced on the S60.         |                                                                                                                                                                                                                                                                                                                                                                                                    |

**Usage Information**

Because installing an Open Automation package may take time, the installation is performed in the background when the download finishes. A message displays on the console when the installation is complete.

To follow the progress of a package installation, enter the [show packages](#) command.

## package uninstall

S55 S60

S4810 Z9000

MXL Switch

Remove an installed Open Automation package, such as Smart Scripting, from the system.

**Syntax**

**package uninstall** *package-name*

**Parameters**

|                     |                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|
| <i>package-name</i> | Enter the name of an Open Automation automation package, exactly as it appears in the <a href="#">show packages</a> list. |
|---------------------|---------------------------------------------------------------------------------------------------------------------------|

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

|                  |                               |
|------------------|-------------------------------|
| Version 9.2(0.0) | Introduced on the MXL switch. |
| Version 9.0.0.0  | Introduced on the Z9000.      |
| Version 8.3.8.0  | Introduced on the S4810.      |
| Version 8.3.5.1  | Introduced on the S55.        |
| Version 8.3.3.4  | Introduced on the S60.        |

**Usage Information**

When you uninstall an Open Automation package, it is removed from the local flash memory.



Caution: Before you uninstall the Smart Scripting package, you must first stop all scripts that are currently running using the **no script script-name** command.

To follow the progress when uninstalling an Open Automation package installation, enter the [show packages](#) command.

**Related commands**

|                               |                                                               |
|-------------------------------|---------------------------------------------------------------|
| <a href="#">show packages</a> | Display all Open Automation packages installed on the switch. |
|-------------------------------|---------------------------------------------------------------|

# script (run)

S55 S60

S4810 S4820T

Z9000 MXL  
Switch

Run a Perl, Python, or UNIX shell script from the Dell Networking operating system (FTOS) command line interface (CLI).

## Syntax

**script** [**username name**] *script-name* [*script-parameter script-parameter ...*]

## Parameters

|                         |                                                                                                                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>username name</b>    | (Optional) Enter the user name whose read-write privileges is applied when the script runs. A username used to run scripts cannot contain special characters.                                                                                                                   |
| <b>script-name</b>      | Enter the name of the script to run, including the directory path and filename; for example:<br>Perl script: /usr/pkg/scripts/sample_scripts/cmd-server.pl<br>Python script: /usr/pkg/scripts/sample_scripts/DisplayAlarms.py<br>UNIX shell script: /usr/pkg/home/admin/test.sh |
| <b>script-parameter</b> | (Optional) Enter the values of up to three parameters to be applied when the script is run. Enter a blank space between parameter values. For example:<br>script username admin /f10/flash/createVlans.py 1 2                                                                   |

## Defaults

None

## Command Modes

CONFIGURATION

## Command History

|                  |                               |
|------------------|-------------------------------|
| Version 9.2(0.0) | Introduced on the MXL switch. |
| Version 9.0.0.0  | Introduced on the Z9000.      |
| Version 8.3.8.0  | Introduced on the S4810.      |
| Version 8.3.5.1  | Introduced on the S55.        |
| Version 8.3.3.4  | Introduced on the S60.        |

## Usage Information

You can enter the **script (run)** command multiple times to run more than one script at the same time; for example:

```
FTOS(conf)#script username root /usr/pkg/scripts/sample_scripts/
DisplayAlarms.py
FTOS(conf)#script username root /usr/pkg/bin/python /usr/pkg/scripts/
VSNAgent/Xen/hpAgtMain.py
```

When you run a script from the FTOS CLI with the **script (run)** command, you can specify an optional user name to apply the read-write privileges assigned to the user name when the script is run (see [Running Scripts with User Privileges](#)). To configure the username and password use the **username** command. If you do not specify a user name with the **script (run)** command, the script is run with the privileges of the current user.

For information about how to run a script directly from a UNIX shell, refer to [Running a Script from the UNIX Shell](#).

To stop a running script, enter the **no script** *script-name* command

To display the scripts that are currently running, including the scripts you have stopped, enter the [show running-config](#) | [grep](#) command.

## script (stop/resume/kill/unschedule)

**S4810** **S4820T**  
Z9000 MXL  
Switch

Stop, resume, kill, or unschedule a Perl, Python, or UNIX shell script from the FTOS CLI.

**Syntax** `script { stop | resume | kill | unschedule } { script-name script-name | job-id job-id | all }`

### Parameters

|                    |                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>stop</b>        | Enter the keyword <b>stop</b> to stop a script from being run.                                                         |
| <b>resume</b>      | Enter the keyword <b>resume</b> to restart a script that has been stopped.                                             |
| <b>kill</b>        | Enter the keyword <b>kill</b> to end a script from executing.                                                          |
| <b>unschedule</b>  | Enter the keyword <b>unschedule</b> to delete a script that was scheduled in EXEC mode.                                |
| <i>script-name</i> | Enter the keywords <b>script-name</b> followed by the name of the script to be stopped, resumed or killed.             |
| <i>job-id</i>      | Enter the keywords <b>job-id</b> followed by the job identifier of the specific job to be stopped, resumed, or killed. |
| <i>all</i>         | Enter the keyword <b>all</b> to stop, resume, or kill all scripts.                                                     |

**Defaults** None

**Command Modes** EXEC

**Command History** Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000, and MXL Switch.

**Usage Information** Use the keyword **unschedule** only on scripts that are not currently running and that were scheduled using the **script execute** command in EXEC mode.

## script execute (EXEC mode)

**S4810** **S4820T**  
Z9000 MXL  
Switch

Schedule when to trigger scripts to execute.

**Syntax** `script execute script-name start { now | time-date | time } [stop {at time-date | after time}] [args arguments] bg`

To cancel, use the **script unschedule** command.

**Parameters**

|                          |                                                                                                                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>script-name</i>       | Enter the name of the script to be scheduled for execution.                                                                                                                                       |
| <b>start now</b>         | Enter the keywords <b>start now</b> to begin executing the script.                                                                                                                                |
| <b>start time-date</b>   | Enter the keywords <b>start time-date</b> with the time and date in HH:MM format to begin executing the script at a specific time. The date can be the present or a future date.                  |
| <b>start time</b>        | Enter the keywords <b>start</b> with the time in HH:MM format to begin executing the script after a set time.                                                                                     |
| <b>stop at time-date</b> | Enter the keywords <b>stop at</b> with the time and date in HH:MM-MM/DD/YY format to stop executing the script. The date must be a future date.                                                   |
| <b>stop after time</b>   | Enter the keywords <b>stop after</b> followed by the time in HH:MM format to stop executing the script.                                                                                           |
| <b>args arguments</b>    | Enter the keyword <b>args</b> followed by the arguments to be scripted. The maximum length is 64 characters. The arguments can be any number of words within quotes (") and separated by a space. |
| <b>bg</b>                | Enter the keyword <b>bg</b> to schedule scripts to run in the background.                                                                                                                         |

**Defaults**

The script runs in the foreground.

**Command Modes**

EXEC

**Command History**

Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000, and MXL Switch.

**Usage Information**

All times selected follow the system time of the switch. The maximum number of scripts to configure for execution is 50. An error message displays when the limit is exceeded. Only one instance of the script runs at a time. Additional schedules to run the same script are ignored until the running script completes and updates are made to the syslog.

## script execute (CONFIGURATION mode)

**S4810** S4820T

Z9000 MXL  
Switch

Schedule when to trigger scripts to execute.

**Syntax**

**script execute** *script-name* **start** {*now* | *time-date* | *time*} [**repeat** {**days** *day* | **minutes** *minutes* | **weekdays** *weekday*}] [**stop** {**at** *time-date* | **after** *time*}] [**args** *arguments*]

To cancel the script execution, use the **no script execute** command.

**Parameters**

|                        |                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>script-name</i>     | Enter the name of the script to be scheduled for execution.                                                                                                           |
| <b>start now</b>       | Enter the keywords <b>start now</b> to begin executing the script.                                                                                                    |
| <b>start time-date</b> | Enter the keyword <b>start</b> with the time and date in HH:MM format to begin executing the script at a specific time. The date can be the present or a future date. |



|                                       |                                                                                                                                                                                                                                                                           |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>start</b> <i>time</i>              | Enter the keyword <b>start</b> with the time in HH:MM format to begin executing the script after a set time.                                                                                                                                                              |
| <b>repeat weekdays</b> <i>weekday</i> | Enter the keywords <b>repeat weekdays</b> to schedule the script to repeat executing on specific days of the week. Select one of the following values: mon, tue, wed, thu, fri, sat, sun, all.                                                                            |
| <b>repeat days</b> <i>day</i>         | Enter the keywords <b>repeat days</b> followed by the day of the month to schedule how often to repeat the script execution. The range is from 1 to 31. Select one value only. For example, 1 for every first day of the month, 10 for every 10th day of the month.       |
| <b>repeat minutes</b> <i>minutes</i>  | Enter the keywords <b>repeat minutes</b> followed by the number of minutes to schedule how often to repeat the script execution. The range is from 1 to 1440. Select one value only. For example, select 20 to repeat every 20 minutes, 60 for repeating once every hour. |
| <b>stop at</b> <i>time/date</i>       | (Optional) Enter the keywords <b>stop at</b> with the time and date in HH:MM-MM/DD/YY format to stop executing the script. The date must be a future date.                                                                                                                |
| <b>stop after</b> <i>time</i>         | (Optional) Enter the keywords <b>stop after</b> followed by the time in HH:MM format to indicate the time after which the script stops executing. For example, “stop after 00:30” indicates to stop the script execution 30 minutes after the start time.                 |
| <b>args</b> <i>arguments</i>          | Enter the keyword <b>args</b> followed by the arguments to be scripted. The maximum length is 64 characters. The arguments can be any number of words within quotes (“”) and separated by a space.                                                                        |

**Defaults** The script runs in the background.

**Command Modes** CONFIGURATION

**Command History** Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000, and MXL Switch.

**Usage Information** All times selected follow the system time of the switch. The maximum number of scripts to configure for execution is 50. An error message displays when the limit is exceeded. Only one instance of the script runs at a time. Additional schedules to run the same script are ignored until the running script completes and updates are made to the syslog.

## script execute triggered-by

**S4810** S4820T

Z9000, MXL  
Switch

Schedule the script to execute on the occurrence of the configured event.

**Syntax**

**script execute** *script-name* **triggered-by** *event-name* [**args** *arguments*]

To cancel the executing the script by an event, use the **no script execute triggered-by** command.

|                        |                                                                          |                                                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b>      | <i>script-name</i>                                                       | Enter the name of the script to be scheduled for execution.                                                                                                                                        |
|                        | <b>triggered-by</b><br><i>event-name</i>                                 | Enter the keywords <b>triggered-by</b> followed by the event name to associate a script to a defined trigger event.                                                                                |
|                        | <b>args arguments</b>                                                    | Enter the keyword <b>args</b> followed by the arguments to be scripted. The maximum length is 64 characters. The arguments can be any number of words within quotes (“”) and separated by a space. |
| <b>Defaults</b>        | The script runs in the background.                                       |                                                                                                                                                                                                    |
| <b>Command Modes</b>   | CONFIGURATION                                                            |                                                                                                                                                                                                    |
| <b>Command History</b> | Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000, and MXL Switch. |                                                                                                                                                                                                    |

## script get

**S4810** **S4820T**  
Z9000 MXL  
Switch

Copy a script to a switch.

### Syntax

**script get url**

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Parameters</b>        | <b>url</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Enter the keyword <b>url</b> followed by the URL location of the script to download to a switch. |
| <b>Defaults</b>          | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                  |
| <b>Command Modes</b>     | EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                  |
| <b>Command History</b>   | Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000, and MXL Switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                  |
| <b>Usage Information</b> | <p>The following formats are supported: FLASH,FTP, TFTP, HTTP, and SCP. To retrieve the script files, use the following formats:</p> <ul style="list-style-type: none"> <li>flash: Copy from the flash file system (flash://filepath)</li> <li>ftp: Copy from the remote file system (ftp://userid:password@hostip/filepath)</li> <li>http: Copy from the remote file system (http://hostip/filepath)</li> <li>scp: Copy from the remote file system (scp://userid:password@hostip/filepath)</li> <li>tftp: Copy from the remote file system (tftp://hostip/filepath)</li> </ul> |                                                                                                  |

The downloaded files are stored into a dedicated folder (**/usr/pkg/ss-scripts**).

# script list execute

**S4810** S4820T  
Z9000 MXL  
Switch

Configure a list of scripts to be run when the switch is rebooted. The scripts may be run before or after loading the configuration file.

**Syntax** `script list execute list-name {on-boot | network-up}`

To delete the list of scripts for an event, use the **no script list execute** command.

## Parameters

|                   |                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------|
| <i>list-name</i>  | Enter the file name that contains the list of scripts to be executed and the sequence in which the scripts will execute. |
| <b>on-boot</b>    | Enter the keywords <b>on-boot</b> to execute the list of scripts when the system is booted up.                           |
| <b>network-up</b> | Enter the keywords <b>network-up</b> to execute the list of scripts when the network interface comes up.                 |

**Defaults** None

**Command Modes** CONFIGURATION

## Command History

Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000 and MXL Switch.

## Usage Information

The maximum number of lists to configure is 2. In Normal Reload mode, the on-boot list executes before applying configurations; it is not executed in BMP mode. The network list is executed after applying configurations; it executes in BMP and Normal Reload mode.

File contents used in the list name are in the following format:

```
#! list_name
seq 1 script <script_name> [args]
seq 2 script <script_name> [args]
seq 3 script <script_name> [args]
seq 4 script <script_name> [args]
seq 5 script <script_name> [args]
```

# script path

**S4810** S4820T  
Z9000 MXL  
Switch

Configure the path for the script on the switch.

**Syntax** `script path path-name`

To remove the path for the script, use the **no script path** command.

|                          |                           |                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameters</b>        | <i>path-name</i>          | Enter the full path of the location of the script. Specify multiple paths using a colon (:). When initialized, the default path is <b>/user/pkg/ss-scripts/</b> .                                                                                                                                                                     |
| <b>Defaults</b>          | None                      |                                                                                                                                                                                                                                                                                                                                       |
| <b>Command Modes</b>     | CONFIGURATION             |                                                                                                                                                                                                                                                                                                                                       |
| <b>Command History</b>   | Version 9.2(0.0)          | Introduced on the S4810, S4820T, Z9000, and MXL Switch.                                                                                                                                                                                                                                                                               |
| <b>Usage Information</b> |                           | The path can contain a network file system (NFS) mounted directory (defined in the <a href="#">mount nfs</a> CLI command). The path is added to a script search list allowing the system to search all locations for the script name. If the script is in multiple locations, the system uses the first instance of the script found. |
| <b>Related commands</b>  | <a href="#">mount nfs</a> | Set up the folders in the NFS mounted directory.                                                                                                                                                                                                                                                                                      |

## script remove

**S4810** **S4820T**  
Z9000 MXL  
Switch

Remove a script from a switch.

**Syntax** **script remove** { *file-name* | **all** }

|                          |                  |                                                                                            |
|--------------------------|------------------|--------------------------------------------------------------------------------------------|
| <b>Parameters</b>        | <i>file-name</i> | Enter the file name of the script to be removed from the switch.                           |
|                          | <b>all</b>       | Enter the keywords <b>all</b> to remove all files from the dedicated folder on the switch. |
| <b>Defaults</b>          | None             |                                                                                            |
| <b>Command Modes</b>     | EXEC             |                                                                                            |
| <b>Command History</b>   | Version 9.2(0.0) | Introduced on the S4810, S4820T, Z9000, and MXL Switch.                                    |
| <b>Usage Information</b> |                  | The files are removed from the folder <b>/usr/pkg/ss-scripts</b> on the switch.            |

## script trigger-event

**S4810** **S4820T**  
Z9000 MXL  
Switch

Configure the event that causes the script to execute.

**Syntax** `script trigger-event event-name {log-event {tag tag} | severity severity level | time-event time | cpu-usage percentage | mem-usage percentage}`

To delete the trigger event, use the **no script trigger-event** command.

**Parameters**


|                                          |                                                                                                                                                                                                                                                |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>event-name</b>                        | Enter the name of the script event to be triggered.                                                                                                                                                                                            |
| <b>log-event {tag tag}</b>               | Enter the keywords <b>log-event tag</b> followed by the pattern (tag) in the syslog message to define the trigger event based on the pattern (tag) in the syslog. A maximum three tags can be given. Each tag must be separated by spaces “ ”. |
| <b>log-event severity severity level</b> | Enter the keywords <b>log-event severity</b> followed by the severity level to define a trigger even based on the syslog message severity level. Valid message security levels are from 1 to 6.                                                |
| <b>time-event time</b>                   | Enter the keywords <b>time-event</b> followed by the time in HH:MM (hour-minute) format to define the trigger event based on the time. Scripts associated with this event run every day at the specified time.                                 |
| <b>time-event time date</b>              | Enter the keywords <b>time-event time</b> followed by the time in HH:MM format and then the date in MM/DD/YY format. The associated script is triggered when the event occurs.                                                                 |
| <b>cpu-usage percentage</b>              | Enter the keywords <b>cpu-usage</b> followed by a percentage value between 20 and 90 to define the trigger event based on CPU usage.                                                                                                           |
| <b>mem-usage percentage</b>              | Enter the keywords <b>mem-usage</b> followed by a percentage value between 20 and 90 to define the trigger event based on memory usage.                                                                                                        |

**Defaults** None

**Command Modes** CONFIGURATION

**Command History**  
Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000 and MXL Switch.

**Usage Information**  
The maximum number of scripts you can configure is 20. The maximum number of allowed tag patterns in a log event trigger is three. The tags of the log events must be an exact comparison. The three tags work as logical or any one match. Only one instance of the script runs at a time. Further schedules to run the same script are ignored until the running script completes and updates are made to the syslog.

 **Note:** Before deleting a trigger event, the script *must* be unlinked from the event.

**Related Commands**  
[script execute triggered-by](#) Configure the event that causes the script to execute.

**Example**  
The following examples define triggers for the subsequent log messages: link down pattern, failure pattern, severity 1 logs, and 85% memory consumption.

**Example “link down” pattern in log messages**  
FTOS(conf)# script trigger-event ma\_event log-event tag "Admin state to down: Ma"

**Example  
“failure” pattern  
in log messages**

```
FTOS(conf)# script trigger-event fail_event log-event tag "failure"
```

**Example  
severity 1 log  
messages**

```
FTOS(conf)# script trigger-event severity1_event log-event severity 1
```

**Example  
85% memory  
consumption**

```
FTOS(conf)# script trigger-event memory_event mem-usage 85
```

## show packages

S55 S60

S4810 Z9000

MXL Switch

Display the installed Open Automation packages, including version number and contents.

**Syntax**

**show packages [brief]**

**Parameters**

**brief**

(Optional) Enter the keyword **brief** to display brief information about the package, version, and status of the package in all stack-units.

**Note:** This option is only available on switches that allow stacking.

**Defaults**

None

**Command Modes**

EXEC

EXEC Privilege

**Command  
History**

Version 9.2(0.0) Introduced on the MXL Switch.

Version 9.0.0.0 Introduced on the Z9000.

Version 8.3.8.0 Introduced on the S4810.

Version 8.3.5.1 Introduced on the S55.

Version 8.3.3.4 Introduced on the S60.

**Usage  
Information**

In a stack setup, FTOS automatically synchronizes the software version installed on the master stack unit with the other switches in the stack. Use the **show packages brief** command to view the installed software versions on the stack units.

**Example (show packages)**

```
FTOS# show packages
* Package Name: SMARTSCRIPTS Version: 2.0.0
 Python 2.6.5
 Perl 5.8.8
 Data::Dumper 2.126
 Class::MethodMaker 2.16
 ExtUtils::MakeMaker 6.56
 XML::NamespaceSupport 1.11
 XML::SAX 0.96
 XML::LibXML 1.70
 Compress::Raw::Bzip2 2.027
 Compress::Raw::Zlib 2.027
 IO::Compress 2.027
 URI 1.54
 HTML::Tagset 3.20
 HTML::Parser 3.65
 LWP 5.836
 Net::Telnet 3.03
 OSSP::uuid 1.0602
 UUID 0.02
 version 0.82
 Class::Inspector 1.24
 Task::Weaken 1.03
 Algorithm::Diff 1.1902
 Text::Diff 1.37
 SOAP::Lite 0.712
 Crypt::SSLeay 0.57
 URI::urn::uuid 0.03
 UUID 0.03
 Crypt::SSLeay 0.57
 Net::SNMP 6.0.0
 Net::Telnet::Cisco 1.10

HTTP Server
 mini_httpd 1.19
 Perl and Python function library for Forcel0 SmartScripts
 smartutils 2.0.0
 WebConnect Web UI and CGI scripts
 htdocs 2.0.0
```

**Example (show packages brief)**

In the following example, Unit 0 is the master stack unit and Unit 1 is the standby unit.

```
FTOS#show packages brief

Package Information

Unit Package Name Version Status

0 SMARTSCRIPTS 2.9.9.2 Installed
 nano 2.2.6nb1 Installing
1 SMARTSCRIPTS 2.9.9.2 Installing
 nano 2.2.6nb1 Installing
2 not present
3 not present
4 not present
5 not present
6 not present
7 not present
8 not present
9 not present
10 not present
11 not present
```

## show script

**S4810** **S4820T**

Z9000 MXL  
Switch

Display the stored, scheduled, and running scripts.

### Syntax

**show script {file | process} | [detail]**

### Parameters

|                |                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>file</b>    | Enter the keyword <b>file</b> to list the stored files in the script path. Enter the optional keyword <b>detail</b> to show detailed output of the scripts including job-id, script type, and script status.  |
| <b>process</b> | Enter the keyword <b>process</b> to list the scripts that are scheduled or running. Enter the optional keyword <b>detail</b> to show detailed output of the relevant arguments that are scheduled or running. |
| <b>detail</b>  | (Optional) Enter the keyword <b>detail</b> to show detailed output of the file including CPU %, memory %, next scheduled time, and any script name or relevant arguments.                                     |

### Defaults

None

### Command Modes

EXEC Privilege

### Command History

Version 9.2(0.0) Introduced on the S4810, S4820T, Z9000, and MXL Switch.

## start shell

**S55** **S60**

**S4810** Z9000  
MXL Switch

Start a NetBSD UNIX shell.

### Syntax

**start shell**

### Defaults

None

### Command Modes

EXEC Privilege

### Command History

|                  |                               |
|------------------|-------------------------------|
| Version 9.2(0.0) | Introduced on the MXL Switch. |
| Version 9.0.0.0  | Introduced on the Z9000.      |
| Version 8.3.8.0  | Introduced on the S4810.      |
| Version 8.3.5.1  | Introduced on the S55.        |
| Version 8.3.3.4  | Introduced on the S60.        |

### Usage Information

You must start an NetBSD shell on a switch before you can enter UNIX commands ([Table 7-2](#)) or run a script directly from the shell to invoke FTOS operations (refer to [Running a Script from the UNIX Shell](#)).



After you start a shell, you are prompted to enter a user name and password.

**Related commands**

---

`show packages`

Display all Open Automation packages installed on the switch.

---

## switch script limit

**S4810** S4820T

Z9000 MXL

Switch

Use the switch script limit to control the script that is running based on CPU, memory, or disk IO usage.

**Syntax**

**switch script limit** {*cpu percentage mem percentage disk percentage*}

To return to the default value, use the **no switch script limit** command.

**Parameters**

---

**cpu percentage**

Enter the keyword **cpu** and the maximum percentage limit to suspend and hold scripts for execution. The range is from 20 to 90 percent.

---

**mem percentage**

Enter the keyword **mem** and the maximum percentage limit to suspend and hold scripts for execution. The range is from 20 to 90 percent.

---

**disk percentage**

Enter the keyword **disk** and the maximum percentage limit to suspend and hold scripts for execution. The range is from 20 to 90 percent. Only the /usr/pkg is monitored.

---

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

---

Version 9.2(0.0) Introduced on the S4810, S4820T, Z900,0 and MXL Switch.

---

**Usage Information**

When any maximum percentage limit is reached, all running scripts are suspended; additional scripts are not be scheduled. Scripts begin running when any of the resource limits reaches 10% less than the configured value. Details are entered into the syslog.

## username

**S55** **S60**

**S4810** Z9000

MXL Switch

Configure an additional user name and password to be used only to run scripts on a switch. The user name and password are used to log in to a UNIX shell and apply the read-write privileges assigned to the user name when a script is run.

**Syntax**

**username** *name password password*

To remove the user name and password, enter **no username**.

**Defaults** none

**Parameters**

|                                 |                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>                     | Enter a username to access the UNIX shell. The user name must be less than 16 characters to satisfy the BSD UNIX login requirements. A username used to run scripts cannot contain special characters. |
| <b>password</b> <i>password</i> | Enter a password to access the UNIX shell.                                                                                                                                                             |

**Command Modes**

CONFIGURATION

**Command History**

|                  |                               |
|------------------|-------------------------------|
| Version 9.2(0.0) | Introduced on the MXL Switch. |
| Version 9.0.0.0  | Introduced on the Z9000.      |
| Version 8.3.8.0  | Introduced on the S4810.      |
| Version 8.3.5.1  | Introduced on the S55.        |
| Version 8.3.3.4  | Introduced on the S60.        |

**Usage Information**

When you run a script from the FTOS CLI with the [script \(run\)](#) command, you can specify an optional user name to apply the read-write privileges assigned to the user name when the script is run (see [Running Scripts with User Privileges](#)).

# Programmatic Interface

[Programmatic Interface](#) is downloaded with FTOS and is supported on the **S4810**, **S4820T**, and Z9000 platforms.

## Overview

Programmatic Interface provides a representational state transfer (REST) application programming interface (API) as an integrated part of the Dell Networking operating system (FTOS).

Use the REST API to configure and monitor a switch using an HTTP-based method to send and receive extensible markup language (XML) protocol data units (PDU) to communicate between the server and client. The REST API supports an XML-based implementation that backs RFC 4741, *NETCONF Configuration Protocol*, and RFC 6020, *YANG - a Data Modeling Language for NETCONF* standards. The system handles up to 10 simultaneous REST API requests to configure or monitor Dell Networking devices.

Script writers can use the REST API on switches without having to code individual CLI commands and open telnet connections for each command.

In addition to using the REST API, you can use third-party management tools and other industry-standard management protocols to manage Dell Networking switches.

XML is a standardized, easy-to-read method for read, create, update, and delete functions. The REST API is an HTTP API that supports API functions such as DELETE, PATCH, POST and PUT methods. For more details, refer to RFC 2616, *Hypertext Transfer Protocol - HTTP/1.1*.

## Important Points to Remember

- You must know the management route.
- Enable the REST API from a configuration prompt using the **rest enable** command.
- You cannot delete physical interfaces using Programmatic Interface.
- Port 8008 is a non-secure port used for HTTP; port 8888 is a secure port used for HTTPS.

## Supported Resources

Resources are the uniform resource identifiers (URIs) that identify the data model accessed by the REST API. The REST API supports the following running configuration and operational resource URIs.

### /ftos

Use the **/ftos** resource for configuring interfaces and routing protocol configurations.

```
<data xmlns:y="http://tail-f.com/ns/rest"
 /api/running">
<ftos xmlns="http://www.dell.com/ns/ftos:0.1/root" "/api/running/ftos"/>
<interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces" "/api/running/
if:interfaces"/>
<operations>
<lock "/api/running/_lock"/>
</operations>
</data>
```

### /ftos/router

Use **/ftos/router** to retrieve all routing configurations from the running configuration database.

Example of **/ftos/router** resource:

```
http://<Management IP address>:<port>//api/running/ftos/router
```

### /ftos/router/bgp

Use **/ftos/router/bgp** to retrieve all border gateway protocol (BGP) configurations from the running configuration database.

Example of **/ftos/router/bgp** resource:

```
http://<Management IP address>:<port>/api/running/ftos/router/bgp?deep
```

### bgp-stats

The **bgp-stats** resource is a proprietary Dell Networking version of the draft-ietf-idr-bgp4-mibv2-05 MIB.

Example of BGP NLRI Table retrieval:

```
http://<Management IP address>:<port>/api/operational/
f10BgpM2NlriTable?deep
```

## fp-stats

Use the **fp-stat** resource to get forwarding plane statistics (such as drop and buffer statistics) for the switch.

Example of retrieving BGP NLRI Table:

```
http://<Management IP address>:<port>/api/operational/fp-stats\?deep
```

## if:interfaces

Also use the **if:interfaces** resource for configuring interfaces. It supports the protocols outlined in the IETF internet draft document *draft-ietf-netmod-interfaces-cfg-03*. For more information, refer to <http://tools.ietf.org/html/draft-ietf-netmod-interfaces-cfg-03>.

Use the **if:interfaces** resource to retrieve the **ifindex** number. Use the **ifindex** number to retrieve the statistical information from the **if mib**.

Example:

```
rest 21]$ curl -v -X PATCH -T ie-rate -u admin:admin http://10.42.51.4:8008/
api/running/if:interfaces/interface/%22tengigabitethernet%200/30%22/
rate-interval
* About to connect() to 10.42.51.4 port 8008
* Trying 10.42.51.4... connected
* Connected to 10.42.51.4 (10.42.51.4) port 8008
* Server auth using Basic with user 'admin'
> PATCH /api/running/if:interfaces/interface/%22tengigabitethernet%200/30%22/
rate-interval HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.15.5 (i686-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/
0.9.8b zlib/1.2.3 libidn/0.6.5
> Host: 10.42.51.4:8008
> Accept: */*
> Content-Length: 37
> Expect: 100-continue
>
< HTTP/1.1 100 Continue
< Server: ConfD
< Allow: GET, POST, OPTIONS, HEAD
< Content-Length: 0
< HTTP/1.1 204 No Content
< Server: ConfD
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Date: Tue, 11 Jan 2005 13:51:43 GMT
< Allow: GET, POST, OPTIONS, HEAD
< Content-Length: 0
< Content-Type: text/html
* Connection #0 to host 10.42.51.4 left intact
* Closing connection #0
```

## if-mib

Use the **if-mib** resource URI to convert statistical and operational data from SNMP MIBs into an XML format. It supports the protocols in RFC 2863. For more information about SNMP MIBs, refer to the *FTOS Configuration Guide, Simple Network Management Protocol (SNMP)* chapter and to <http://tools.ietf.org/html/rfc2863>.

## if-mib interfaces

Use the **if-mib:interfaces** resource to retrieve monitoring (operational) status information for interfaces based on the **ifindex** (ifTable).

Example:

```
http://<management IP address>:<port>/api/operational/if-mib:interfaces/
ifEntry/41042946
```

## Retrieving IF Index Information

Interface stats (operational data) are retrievable via the IF MIB.

- This model is indexed by IF Index (per standard definition).

Interface configuration is retrievable via IETF\_Interfaces.yang.

- This model is indexed by name (slot/port) – per NETMOD Draft standard.

The IF Index can be retrieved via the IETF\_INTERFACES table as highlighted in the example below.

```
curl -v -s -u admin:admin http://<Management IP address>:<Port>/api/
operational/if:interfaces/interface/%220/14%22
(...)
<interface /api/operational/if:interfaces/interface/%220/14%22"
xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces" xmlns:y="http://
tail-f.com/ns/rest" xmlns:if="urn:ietf:params:xml:ns:yang:ietf-interfaces"
y:path="/if:interfaces/if:interface%5Bif:name%3D%220/14%22%5D">
 <name>0/14</name>
 <description></description>
 <type>ethernetCsmacd</type>
 <location>Te 0/14</location>
 <enabled>true</enabled>
 <if-index>37291010</if-index>
</interface>
* Connection #0 to host 10.11.200.41 left intact
* Closing connection #0
```

Use the retrieved IF Index to retrieve the operational data.

```
curl -v -s -u admin:admin http://<Management IP address>:<Port>/api/
operational/if-mib:interfaces/ifEntry/37291010
(...)

<ifEntry /api/operational/if-mib:interfaces/ifEntry/37291010"
xmlns="urn:ietf:params:xml:ns:yang:smiv2:IF-MIB" xmlns:y="http://tail-f.com/
ns/rest" xmlns:if-mib="urn:ietf:params:xml:ns:yang:smiv2:IF-MIB" y:path="/
if-mib:interfaces/if-mib:ifEntry%5Bif-mib:ifIndex%3D%2237291010%22%5D">
 <ifIndex>37291010</ifIndex>
 <ifDescr>TenGigabitEthernet 0/14</ifDescr>
 <ifType>ethernetCsmacd</ifType>
 <ifMtu>1554</ifMtu>
 <ifSpeed>1000000000</ifSpeed>
 <ifPhysAddress>00:01:e8:8c:4d:12</ifPhysAddress>
 <ifAdminStatus>up</ifAdminStatus>
 <ifOperStatus>up</ifOperStatus>
 <ifLastChange>18910</ifLastChange>
 <ifInOctets>0</ifInOctets>
 <ifInUcastPkts>0</ifInUcastPkts>
 (etc...)
</ifEntry>
* Connection #0 to host 10.11.200.41 left intact
* Closing connection #0
```

## REST Authentication

To enable the AAA accounting model (Accounting, Authentication, and Authorization), the REST API must be authenticated on FTOS. For more information about the AAA accounting mode, refer to the *FTOS Configuration Guide, Security* chapter.

The FTOS CLI user level privilege dictates the level of the REST API access. Users with privilege level 0 or 1 have read-only access; the allowed REST API method is GET. Users with privilege levels 2 through 15 have read-write access in REST API. The allowed methods are GET, PATCH, PUT, POST, and DELETE.

For information about the **privilege level** command, refer to the *FTOS Command Line Reference Guide, Security* chapter.

## Configuring a BGP Network Topology

In this release, the REST API supports a finite number of features including Forwarding Plane Statistics, BGP monitoring, Interface statistics, partial Interface configuration, and partial BGPv4 configuration.

The following example shows a typical external border gateway protocol (EBGP) network topology where a Z9000 is the core spine between a leaf S4810 and an upstream autonomous system boundary router (ASBR).

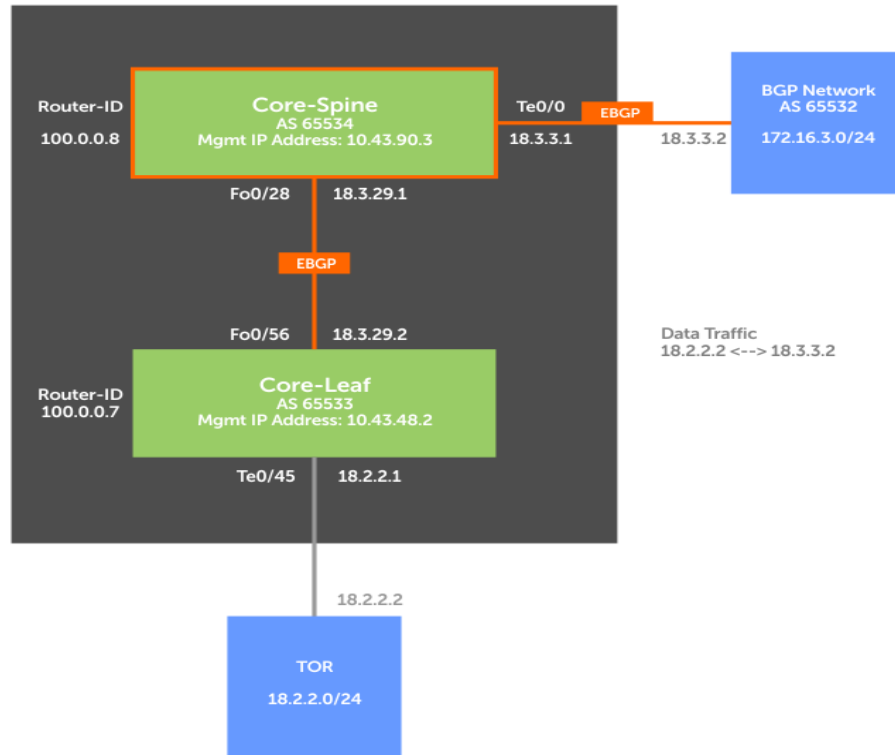


Figure 11-1. Typical Spine/Leaf Network Topology

## Configure the Physical Interfaces

Use Programmatic Interface to modify the following physical interface attributes:

- Enable/Disable the interface
- IP (address)
- Description
- MTU
- Rate-interval



**Note:** You cannot delete physical interfaces using Programmatic Interface.



The examples in this section were created using CURL which is a utility that allows data to be transferred using various protocols. The following options are used in the following CURL examples.

- -s indicates silent mode.
- -v indicates verbose mode. Commands used with this mode will give details of all the HTTP requests being sent and received from the Dell Networking switch.
- -u indicates user.



**Note:** The “%22” in the following output examples is the ASCII HTML character for quotation marks ( “ ) and is specific to the CURL utility in which the output examples were created.

On a 10G Ethernet interface, you can modify the physical interface attributes using Programmatic Interface as shown in the following example:

```
<interface>
 <tengigabitethernet>
 <name>0/0</name>
 <ip>
 </ip>
 <rate-interval>299</rate-interval>
 <mtu>1554</mtu>
 <shutdown>true</shutdown>
 </tengigabitethernet>
</interface>
```

Following are the URIs provided to manage physical interfaces.

To retrieve all the sub-resources of the query, use `deep` in the URI request query. To retrieve the query data without the sub-resources, use `shallow`.

These are the attributes:

- interface
  - /running/ftos/interface/fortyGigE/%220/28%22
  - /running/ftos/interface/tengigabitethernet/%220/0%22
- operational
  - /operational/if:interfaces/interface/%22fortyGigE%200/28%22
  - /operational/if-mib:interfaces/\?deep
  - /operational/if-mib:interfaces/ifEntry/41042946

Configure the physical links from the core to the leaf and upstream ASBR.

Configure the physical link from the spine Z9000 to the leaf as follows. (The following example uses a CURL utility.)

```
curl -s -u admin:admin -X PATCH -T patch_phy_40g
http://<Management IP address>:<Port>/api/running/ftos/interface/fortyGigE/
%220/28%22
```

Where `patch_phy_40g` is the patch file that contains the XML used to configure the interface.

Following is an example of how to configure the physical interfaces (IP address, MTU, rate-interval, and no shutdown) on a 40G port:

```
XML file - patch_phy_40g

<fortyGigE>
 <mtu>9252</mtu>
 <rate-interval>30</rate-interval>
 <ip>
 <address>
 <primary>
 <address>18.3.29.1/30</address>
 </primary>
 </address>
 </ip>
 <shutdown>false</shutdown>
</fortyGigE>
```

Configure the physical link from the spine Z9000 to the upstream router as follows:

```
curl -s -u admin:admin -X PATCH -T patch_phy_10g
http://<Management IP address>:<Port>/api/running/ftos/interface/
tengigabitethernet/%220/0%22
```

## Review Interface Configurations and Statistics

To view what is configured on the system, use the following commands. To show the top-level uniform resource identifier (URI) resources, enter:

```
api
```

To get the running configuration, enter:

```
/api/running/ftos\?deep
```

To view the configuration for a 40G interface on the spine, enter:

```
api/running/ftos/interface/fortyGigE/%220/28%22
```

To view the configuration for a 10G interface on the leaf, enter:

```
api/running/ftos/interface/tengigabitethernet/%220/0%22
```

Read the configuration via a data model proposed by standard body; for example, ietf-interfaces.

```
api/operational/if:interfaces/interface/%22fortyGigE%200/28%22
```

Read the operational statistic data for a data model converted from simple network management protocol (SNMP) MIBs, such as IF-MIB.

```
api/operational/if-mib:interfaces/\?deep
```

To find the ifIndex of a physical interface by ietf-interfaces, enter:

```
api/operational/if:interfaces/interface/%22fortyGigE%200/28%22
```

To get the operational data of a physical interface by ifIndex, enter:

```
/api/operational/if-mib:interfaces/ifEntry/
```

## POST and GET Request Examples

The following output displays a POST request to create BGP 65009:

```
linux:~/REST$ cat HTTP_SEND_post_bgp
<bgp>
 <as-name>65009</as-name>
 <maximum-paths>
 <ebgp>64</ebgp>
 <ibgp>32</ibgp>
 </maximum-paths>
</bgp>
linux:~/REST$ curl -v -u admin:admin -X POST -T HTTP_SEND_post_bgp http://
10.43.48.2:8008/api/running/ftos/router
* About to connect() to 10.43.48.2 port 8008 (#0)
* Trying 10.43.48.2... connected
* Server auth using Basic with user 'admin'
> POST /api/running/ftos/router HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.22.0 (i686-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1
zlib/1.2.3.4 libidn/1.23 librtmp/2.3
> Host: 10.43.48.2:8008
> Accept: */*
> Content-Length: 118
> Expect: 100-continue
>
< HTTP/1.1 100 Continue
< Server: ConfD
< Allow: GET, POST, OPTIONS, HEAD
< Content-Length: 0
* We are completely uploaded and fine
< HTTP/1.1 204 No Content
< Server: ConfD
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Date: Thu, 01 Aug 2013 21:42:46 GMT
< Allow: GET, POST, OPTIONS, HEAD
< Content-Length: 0
< Content-Type: text/html
<
* Connection #0 to host 10.43.48.2 left intact
* Closing connection #0
```

The following output displays a GET request after running the POST request using CURL:

```
linux:~/REST$ curl -v -u admin:admin http://10.43.48.2:8008/api/running/ftos/
router/bgp
* About to connect() to 10.43.48.2 port 8008 (#0)
* Trying 10.43.48.2... connected
* Server auth using Basic with user 'admin'
> GET /api/running/ftos/router/bgp HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.22.0 (i686-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1
zlib/1.2.3.4 libidn/1.23 librtmp/2.3
> Host: 10.43.48.2:8008
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: ConfD
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Date: Thu, 01 Aug 2013 21:50:48 GMT
< Content-Type: application/vnd.yang.data+xml
< Transfer-Encoding: chunked
<

<bgp>
 <as-name>65009</as-name>
 <timers>
 <bgp>
 <keepalive>60</keepalive>
 <hold-time>180</hold-time>
 </bgp>
 </timers>
 <maximum-paths>
 <ebgp>64</ebgp>
 <ibgp>32</ibgp>
 </maximum-paths>
</bgp>
* Connection #0 to host 10.43.48.2 left intact
* Closing connection #0
```

## Available Resource Paths

To configure the interfaces and BGP and view statistical data, use the following resource paths.

To access statistical resources, attach the resource path to the operational base URL. For example, to use `fp-stats`, enter `http://<Management IP address>:<Port>/api/operational/fp-stats\?deep`.

To access configuration resources, attach the resource path to the FTOS running base URL. For example, to use `interface`, enter `http://<Management IP address>:<Port>/api/running/ftos/interface`.

In FTOS version 9.2(0.0), the following important points are true:

- In the case of forwarding plane statistics for stacked units, the stack unit number is passed as an input parameter.
- Interface Configuration support is provided for physical interfaces only.

| <b>Forwarding Plane Statistics</b>                |
|---------------------------------------------------|
| <code>fp-stats</code>                             |
| Get data plane statistics.                        |
| <code>fp-cpu-party-bus-stats</code>               |
| Get management plane statistics                   |
| <code>fp-drops</code>                             |
| Get management port statistics                    |
| <code>fp-drops</code>                             |
| Get drop statistics per stack-unit                |
| <code>fp-drops</code>                             |
| Get drop statistics per port                      |
| <code>fp-packet-buffer</code>                     |
| Get buffer statistics per stack unit              |
| <code>fp-packet-buffer</code>                     |
| Get buffer statistics per port                    |
| <code>fp-port-stats</code>                        |
|                                                   |
| <b>BGP Statistics</b>                             |
| <code>f10BgpM2NlriTable</code>                    |
| Get BPG IPv4 routing table for the system         |
| <code>f10BgpM2PathAttrCommTable</code>            |
| Get BGP routes with community attributes          |
| <code>f10BgpM2NlriTable</code>                    |
| Get BGP routes that are dampened/non-active       |
| <code>f10BgpM2PathAttrExtCommTable</code>         |
| Get BGP routes with extended community attributes |
| <code>f10BgpM2FlapStatisticsTables</code>         |
| Get flap-statistics on BGP routes                 |
| <code>f10BgpM2PeerTable</code>                    |
| Get BGP neighbors info                            |
| <code>f10BgpM2PathAttrTable</code>                |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Get BGP next-hops                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>f10BgpM2PathAttrTable</code>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Get all BGP paths                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>f10BgpM2AsPathTable</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Get all unique BGP AS-PATHs                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>f10BgpM2PeerTable</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Get all peers in a peer-group                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>f10BgpM2PeerTable</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Interface Statistics</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>if:interfaces</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Get interface statistics                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <code>if-mib:interfaces</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Interface Configuration</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>interface</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>Modify interface properties:</p> <ul style="list-style-type: none"> <li>• Enable/Disable</li> <li>• IP (address)</li> <li>• Description</li> <li>• MTU</li> <li>• Rate-interval</li> </ul>                                                                                                                                                                                                                                                                                   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>BGPv4 Configuration</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>router/bgp</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>For information about the corresponding CLI command, refer to the <b>bgp confederation identifier</b> command in the <i>FTOS Command Line Reference Guide, Border Gateway Protocol (BGP)</i> chapter.</p> <p>Specify the AS number for ROUTER BGP.</p> <p>Enable BGP routing on an IP Network.</p> <p>Configure the BGP keep alive interval.</p> <p>Enable multiple parallel paths.</p> <p>Configure neighbor remote-as, description.</p> <p>Shut down the BGP neighbor.</p> |

# HTTP Status Error Codes

The REST API server returns the following HTTP status error codes:

|                                   |                                                                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>200 OK</b>                     | The request was successfully completed. A response body is returned containing a representation of the resource.                                                         |
| <b>201 Created</b>                | A resource was created and the new resource URI is returned in the “Location” header.                                                                                    |
| <b>204 No Content</b>             | The request was successfully completed, but no response body is returned.                                                                                                |
| <b>400 Bad Request</b>            | The request could not be processed because it contains missing or invalid information (such as validation error on an input field, a missing required value, and so on). |
| <b>401 Unauthorized</b>           | The request requires user authentication. The response includes a “WWW-Authenticate” header field for basic authentication.                                              |
| <b>403 Forbidden</b>              | Access to the resource was denied by the server due to authorization rules.                                                                                              |
| <b>404 Not Found</b>              | The requested resource does not exist.                                                                                                                                   |
| <b>405 Method Not Allowed</b>     | The HTTP method specified in the request (DELETE, GET, HEAD, PATCH, POST, PUT) is not supported for this resource.                                                       |
| <b>406 Not Acceptable</b>         | The resource identified by this request is not capable of generating the requested representation, specified in the “Accept” header or in the “format” query parameter.  |
| <b>409 Conflict</b>               | This code is used if a request tries to create a resource that already exists.                                                                                           |
| <b>415 Unsupported Media Type</b> | The format of the request is not supported.                                                                                                                              |
| <b>500 Internal Error</b>         | The server encountered an unexpected condition which prevented it from fulfilling the request.                                                                           |
| <b>501 Not Implemented</b>        | The server does not (currently) support the functionality required to fulfill the request.                                                                               |
| <b>503 Unavailable</b>            | The server is currently unable to handle the request due to the resource being used by someone else or is temporarily overloaded.                                        |



# Elements of REST API XML Attributes

The following describe the elements of the REST API XML attributes.

## ip address - Primary / Secondary

### Description

Assign a primary or secondary IP address to a physical interface.

### Usage (via HTTP Patch)

```
<ftos>
 <interface>
 <tengigabitethernet>
 <name>0/1</name>
 <ip>
 <address>
 <primary>
 <address>1.2.3.4/24</address>
 </primary>
 <secondary>
 <address>1.2.3.6/24</address>
 </secondary>
 </address>
 </ip>
 </tengigabitethernet>
 </interface>
</ftos>
```

## shutdown

### Description

Specify whether a physical interface is enabled or disabled.

### Usage (via HTTP Patch)

```
<ftos>
 <interface>
 <tengigabitethernet>
 <name>0/1</name>
 <shutdown>true</shutdown>
 </tengigabitethernet>
 </interface>
</ftos>
```

# Border Gateway Protocol

The examples in the following section relate to border gateway protocol (BGP). Use the following example to access BGP from the REST API.

```
<router>
 <bgp>
 <as-name>1</as-name>
 </bgp>
</router>
```

## bgp neighbor

**Description** Manage the BGP neighbor attributes.

### create

**Description** Create a BGP neighbor.

**Usage (via HTTP Create)**

```
<router>
 <bgp>
 <as-name>1</as-name>
 <neighbor>
 <neighbor-router>3.3.3.3</neighbor-router>
 <remote-as>64555</remote-as>
 <shutdown>true</shutdown>
 </neighbor>
 </bgp>
</router>
</ftos>
```

**Attributes** **Neighbor-router:** Specify the neighbor router (IP address).

**Remote-as:** Specify the remote autonomous system.

**Shutdown:** Enable/disable state of the neighbor.

## delete

**Description** Specify the URI of the BGP neighbor to be deleted.

**Usage (via HTTP delete)** <http://<Management IP>:<Port>/api/running/ftos/router/bgp/<AS number>/neighbor/<Neighbor IP>>

## bgp network

**Description** Specify the networks for the BGP process and enter them into the BGP routing table.

**Usage**

```
<router>
 <bgp>
 <as-name>1</as-name>
 <network>
 <ipv4-address>4.4.0.0/16</ipv4-address>
 </network>
 </bgp>
```

## bgp timers

**Description** Set the keepalive and hold time timers for BGP.

**Usage**

```
<router>
 <bgp>
 <as-name>1</as-name>
 <timers>
 <bgp>
 <keepalive>60</keepalive>
 <hold-time>180</hold-time>
 </bgp>
 </timers>
 </bgp>
</router>
```

## bgp maximum paths

**Description** Configure the maximum number of parallel routes (multipath support) that BGP supports.

## Usage

```
<router>
 <bgp>
 <as-name>1</as-name>
 <maximum-paths>
 <ebgp>1</ebgp>
 <ibgp>1</ibgp>
 </maximum-paths>
 </bgp>
</router>
```

# Programmatic Interface CLI

## Overview

Programmatic Interface CLI commands are supported on the **S4810** S4820T and **Z** platforms.

The following commands are supported.

### rest enable

**S4810** S4820T

**Z**

Enable the REST interface to.

To return to the default value, use the **no rest enable** command.

**Syntax**

**rest enable**

**Defaults**

REST is disabled by default.

**Command Modes**

CONFIGURATION

**Command History**

---

Version 9.2(0.0) Introduced on the S4810, S4820T, and Z9000.

---

**Usage Information**

The REST Interface grants access to the Programmatic Interface feature. To view interface statistics, forwarding plane, and BGP statistical information, use Programmatic Interface.



# Programmatic Interface REST API Commands

## Overview

Programmatic Interface REST API commands are supported on the **S4810**, **S4820T**, and Z9000 platforms.

Refer to the *Programmatic Interface* chapter in the *Open Automation Guide* for information on resources (URIs) supported by REST API.

The following REST API commands are supported.

**interface / {tengigabitethernet | fortyGigE }**  
Configure an Ethernet resource.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Platforms</b>  | <b>S4810</b> <b>S4820T</b> Z9000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Example</b>    | <pre> &lt;interface&gt;   &lt;tengigabitethernet&gt;     &lt;name&gt;0/0&lt;/name&gt;     &lt;ip&gt;       &lt;/ip&gt;     &lt;rate-interval&gt;299&lt;/rate-interval&gt;     &lt;mtu&gt;1554&lt;/mtu&gt;     &lt;shutdown&gt;true&lt;/shutdown&gt;   &lt;/tengigabitethernet&gt;   &lt;tengigabitethernet&gt;     &lt;name&gt;0/1&lt;/name&gt;     &lt;ip &gt;       &lt;address &gt;         &lt;primary&gt;           &lt;address&gt;1.2.3.4/24&lt;/address&gt;         &lt;/primary&gt;       &lt;/address&gt;     &lt;/ip&gt;     &lt;rate-interval&gt;299&lt;/rate-interval&gt;     &lt;mtu&gt;1554&lt;/mtu&gt;     &lt;shutdown&gt;true&lt;/shutdown&gt;   &lt;/tengigabitethernet&gt; &lt;/interface&gt; </pre> |
| <b>Attributes</b> | <ul style="list-style-type: none"> <li>description</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

- interface
- ip
- name
- mtu
- rate-interval
- shutdown

For more information on the REST API command parameters, refer to the *FTOS Command Line Reference Guide, Interfaces* chapter.

## router/bgp/as-name

Enter the autonomous system (AS) name.

**Platforms** **S4810** S4820T Z9000

**Example**

```
<router>
 <bgp>
 <as-name>1</as-name>
 </bgp>
</router>
```

**Attributes**

- as-name

For more information on the REST API command parameters, refer to the *FTOS Command Line Reference Guide, Border Gateway Protocol* chapter.

## /router/bgp/network/ipv4-address

Set the BGP IPv4 address on the network.

**Platforms** **S4810** S4820T Z9000

**Example**

```
<network>
 <ipv4-address>1.1.1.1/32</ipv4-address>
</network>
```

**Attributes**

- ipv4-address

For more information on the REST API command parameters, refer to the *FTOS Command Line Reference Guide, Border Gateway Protocol* chapter.

## /router/bgp/timers/bgp

Adjust the BGP Keep Alive and Hold Time timers.

**Platforms** **S4810** S4820T Z9000

**Example** <timers>



```
<bgp>
 <keepalive>60</keepalive>
 <hold-time>180</hold-time>
</bgp>
</timers>
```

- Attributes**
- [keepalive](#)
  - [holdtime](#)

For more information on the REST API command parameters, refer to the *FTOS Command Line Reference Guide, Border Gateway Protocol* chapter.

## /router/bgp/maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

**Platforms** **S4810** **S4820T** Z9000

**Example**

```
<maximum-paths>
 <ebgp>1</ebgp>
 <ibgp>1</ibgp>
</maximum-paths>
```

- Attributes**
- [ebgp](#)
  - [ibgp](#)

For more information on the REST API command parameters, refer to the *FTOS Command Line Reference Guide, Border Gateway Protocol* chapter.

## /router/bgp/neighbor

Assign a character string describing the neighbor or group of neighbors (peer group).

**Platforms** **S4810** **S4820T** Z9000

**Example**

```
<neighbor>
 <neighbor-router>3.3.3.3</neighbor-router>
 <remote-as>64555</remote-as>
 <shutdown>true</shutdown>
</neighbor>
```

- Attributes**
- [neighbor-router](#)
  - [remote-as](#)
  - [description](#)
  - [shutdown](#)

For more information on the REST API command parameters, refer to the *FTOS Command Line Reference Guide, Border Gateway Protocol* chapter.



## Web Server with HTTP Support

Web Server with HTTP Support are downloaded with the SmartScripts package (see [Downloading the Smart Scripting Package](#)). It is supported on the [S55](#) [S60](#) [S4810](#) [S4820T](#) Z9000, and MXL Switch platforms.

This chapter describes the Web-based components in the Open Automation package:

- [Web Server](#)

### Web Server

In the Open Automation package, the web server runs on a switch and handles HTTP and HTTPS requests. You can start the web server in a non-secure (HTTP) or secure (HTTPS) mode.

To start the web server in a non-secure (without SSL) mode for receiving HTTP requests and write the configuration to the running configuration, enter the following **http-server http** command.

| Command Syntax          | Command Mode  | Task                                                                           |
|-------------------------|---------------|--------------------------------------------------------------------------------|
| <b>http-server http</b> | CONFIGURATION | Starts the web-server application in non-secure mode to receive HTTP requests. |

**Note:** The Dell Networking operating system (FTOS) uses port 80 for S4810, S4820T, and Z9000. FTOS uses port 8080 for the MXL Switch.

To start the web server in a secure mode for receiving HTTPS requests and write the configuration to the running configuration, enter the **http-server secure-http** command:

| Command Syntax                 | Command Mode  | Task                                                                                  |
|--------------------------------|---------------|---------------------------------------------------------------------------------------|
| <b>http-server secure-http</b> | CONFIGURATION | Starts the web-server application in secure mode using SSL to receive HTTPS requests. |

Enter the **no http-server {http | secure-http}** command to stop the web server and remove the configuration from the running-configuration file.



# Web Graphical User Interface

This appendix contains examples of the output displayed for each menu option in the Web interface used in the Open Automation Framework for the menus:

- System
- Interfaces
- Protocols
- Diagnostics
- Utilities
- Settings

---

## System Menu

---

### System > Software Version

#### SOFTWARE VERSION

---

```
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: E8-3-10-101
Copyright (c) 1999-2011 by Force10 Networks, Inc.
Build Time: Tue Oct 25 00:45:41 PDT 2011
Build Path: /sites/sjc/work/build/buildSpaces/build09/E8-3-10/SW/SRC/Cp_src/Tacacs
Force10 uptime is 1 hour(s), 0 minute(s)
```

```
System image file is "/tftpboot/arir/FTOS-SE-8-3-10-101.bin"
```

```
System Type: S4810
Control Processor: Freescale QorIQ P2020 with 2147483648 bytes of memory.
```

```
128M bytes of boot flash memory.
```

```
1 52-port GE/TE/FG (SE)
48 Ten GigabitEthernet/IEEE 802.3 interface(s)
4 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

---

### System > Time/Date

#### CURRENT DATE

---

```
03:09:46.883 PST Sat Nov 12 2011
```

---

### System > Memory Usage

#### MEMORY USAGE

---

```
Statistics On Unit 0 Processor
=====
Total (b) Used (b) Free (b) Lowest (b) Largest (b)
2147483648 3825202 2143658446 2143641882 2143658446
```

## System &gt; CPU Usage

## CPU USAGE

## CPU Statistics Of Unit 0

=====

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

| PID        | Runtime (ms) | Invoked | uSecs | 5Sec  | 1Min  | 5Min  | TTY | Process             |
|------------|--------------|---------|-------|-------|-------|-------|-----|---------------------|
| 0x42caa000 | 60           | 6       | 10000 | 0.00% | 0.00% | 0.00% | 0   | diagagt             |
| 0x42c88000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | debugagt            |
| 0x42c67000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | F10StkMgr           |
| 0x42c44000 | 8240         | 824     | 10000 | 0.00% | 0.00% | 0.02% | 0   | lcMgr               |
| 0x42c1e000 | 20           | 2       | 10000 | 0.00% | 0.00% | 0.00% | 0   | dla                 |
| 0x42bf9000 | 440          | 44      | 10000 | 0.00% | 0.00% | 0.00% | 0   | sysAdmTsk           |
| 0x42bd8000 | 3070         | 307     | 10000 | 0.00% | 0.00% | 0.00% | 0   | timerMgr            |
| 0x42bb5000 | 5880         | 588     | 10000 | 0.00% | 0.00% | 0.00% | 0   | PM                  |
| 0x42b91000 | 6200         | 620     | 10000 | 0.00% | 0.00% | 0.00% | 0   | KP                  |
| 0x42b6e000 | 10           | 1       | 10000 | 0.00% | 0.00% | 0.00% | 0   | evagt               |
| 0x42b48000 | 250          | 25      | 10000 | 0.00% | 0.00% | 0.00% | 0   | ipc                 |
| 0x41e1e000 | 210          | 21      | 10000 | 0.00% | 0.00% | 0.00% | 0   | tme                 |
| 0x41e1c000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | ttraceIpFlow        |
| 0x41e19000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | linkscan_user_threa |
| 0x41df9000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | tDDB                |
| 0x41df6000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | GC                  |
| 0x41df2000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | isrTask             |
| 0x41de9000 | 30           | 3       | 10000 | 0.00% | 0.00% | 0.00% | 0   | bshell_reaper_threa |
| 0x41de0000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | tSysLog             |
| 0x41dde000 | 420          | 42      | 10000 | 0.00% | 0.00% | 0.00% | 0   | tTimerTask          |
| 0x41ddc000 | 7630         | 763     | 10000 | 0.00% | 0.00% | 0.00% | 0   | tExcTask            |
| 0x41dca000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | tLogTask            |
| 0x41dc4000 | 43120        | 4312    | 10000 | 0.00% | 0.00% | 0.00% | 0   | tUsrRoot            |
| 0x41d80000 | 10           | 1       | 10000 | 0.00% | 0.00% | 0.00% | 0   | main                |
| 0x43147000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | tFib6audit          |
| 0x42f95000 | 170          | 17      | 10000 | 0.00% | 0.00% | 0.00% | 0   | igmpAgent           |
| 0x42f92000 | 100          | 10      | 10000 | 0.00% | 0.00% | 0.00% | 0   | tFib6spf            |
| 0x42f60000 | 16850        | 1685    | 10000 | 0.00% | 0.08% | 0.03% | 0   | l2LrnAgeMove        |
| 0x42efe000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | fib6                |
| 0x42ed3000 | 1300         | 130     | 10000 | 0.00% | 0.00% | 0.00% | 0   | MacAgent            |
| 0x42eb1000 | 11400        | 1140    | 10000 | 0.00% | 0.00% | 0.02% | 0   | frrpagt             |
| 0x42e7b000 | 700          | 70      | 10000 | 0.00% | 0.00% | 0.00% | 0   | dsagt               |
| 0x42e58000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | tFib4audit          |
| 0x42d7c000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | ifaDispatch         |
| 0x42d62000 | 5750         | 575     | 10000 | 0.00% | 0.00% | 0.00% | 0   | ifagt_1             |
| 0x42d25000 | 130          | 13      | 10000 | 0.00% | 0.00% | 0.00% | 0   | tFib4spf            |
| 0x42d23000 | 330          | 33      | 10000 | 0.00% | 0.00% | 0.00% | 0   | aclAgent            |
| 0x42cf9000 | 10           | 1       | 10000 | 0.00% | 0.00% | 0.00% | 0   | tFib4               |
| 0x42c42000 | 90           | 9       | 10000 | 0.00% | 0.00% | 0.00% | 0   | count               |
| 0x4336e000 | 0            | 0       | 0     | 0.00% | 0.00% | 0.00% | 0   | frrpaRecv           |

---

## System > Boot Variables

### BOOT VARIABLES

```
PRIMARY IMAGE FILE = tftp://10.42.7.77/tftpboot/arir/FTOS-SE-8-3-10-101.bin
SECONDARY IMAGE FILE = system://A
DEFAULT IMAGE FILE = system://A
LOCAL CONFIG FILE = variable does not exist
PRIMARY HOST CONFIG FILE = variable does not exist
SECONDARY HOST CONFIG FILE = variable does not exist
PRIMARY NETWORK CONFIG FILE = variable does not exist
SECONDARY NETWORK CONFIG FILE = variable does not exist
CURRENT IMAGE FILE = tftp://10.42.7.77/tftpboot/arir/FTOS-SE-8-3-10-101.bin
CURRENT CONFIG FILE 1 = flash://startup-config
CURRENT CONFIG FILE 2 = variable does not exist
CONFIG LOAD PREFERENCE = local first
BOOT INTERFACE GATEWAY IP ADDRESS = 0.0.0.0
Reload Mode = normal-reload
```

---

## System > Running Config

### RUNNING CONFIG

```
Current Configuration ...
! Version E8-3-5-58
! Last configuration change at Thu Sep 29 17:58:15 2011 by admin
! Startup-config last updated at Tue Sep 20 00:10:37 2011 by admin
!
boot system stack-unit 0 primary tftp://10.42.7.77/FTOS-SD-8-3-5-58.bin
boot system stack-unit 0 secondary system: A:
boot system stack-unit 0 default tftp://10.42.7.77/FTOS-SD-8-3-5-58.bin
boot system gateway 10.43.0.1
!
redundancy auto-synchronize full
!
hardware watchdog
!
hostname st-s55-0a
!
enable password 7 b125455cf679b208e79b910e85789edf
!
username test password 7 7b56aef7d3a1cce8
username admin password 7 1d28e9f33f99cf5c
username admin1 password 7 3b0067cc6673eaec
!
protocol spanning-tree mstp
no disable
!
stack-unit 0 provision S55
!
interface GigabitEthernet 0/0
no ip address
shutdown
!
interface GigabitEthernet 0/1
no ip address
switchport
no shutdown
!
```

---

## System > Information

### SYSTEM INFORMATION

---

Hostname ..... Force10  
IP address ..... 10.42.51.5/16  
FTOS Version ..... E8-3-10-101  
Platform ..... S4810  
Uptime ..... 57 minute(s)  
Last config change ..... Tue Nov 8 12:52:54 2011 by admin

---



## Interfaces Menu

### Interfaces > All

| ALL INTERFACES         |              |     |        |                       |          |      |  |
|------------------------|--------------|-----|--------|-----------------------|----------|------|--|
| Interface              | IP-Address   | OK  | Method | Status                | Protocol |      |  |
| GigabitEthernet 0/0    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/1    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/2    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/3    | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/4    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/5    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/6    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/7    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/8    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/9    | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/10   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/11   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/12   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/13   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/14   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/15   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/16   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/17   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/18   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/19   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/20   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/21   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/22   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/23   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/24   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/25   | unassigned   | NO  | Manual | up                    |          | down |  |
| GigabitEthernet 0/26   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/27   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/28   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/29   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/30   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/31   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/32   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/33   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/34   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/35   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/36   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/37   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/38   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/39   | 39.39.39.2   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/40   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/41   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/42   | unassigned   | YES | Manual | up                    |          | up   |  |
| GigabitEthernet 0/43   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/44   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/45   | 70.70.70.1   | NO  | Manual | up                    |          | down |  |
| GigabitEthernet 0/46   | unassigned   | NO  | Manual | administratively down | down     | down |  |
| GigabitEthernet 0/47   | unassigned   | NO  | Manual | up                    |          | down |  |
| ManagementEthernet 0/0 | 10.43.60.100 | YES | Manual | up                    |          | up   |  |

## Interfaces > Physical

### PHYSICAL INTERFACES

| Interface            | IP-Address | OK  | Method | Status                | Protocol |
|----------------------|------------|-----|--------|-----------------------|----------|
| GigabitEthernet 0/0  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/1  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/2  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/3  | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/4  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/5  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/6  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/7  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/8  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/9  | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/10 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/11 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/12 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/13 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/14 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/15 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/16 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/17 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/18 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/19 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/20 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/21 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/22 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/23 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/24 | unassigned | YES | Manual | up                    | up       |
| GigabitEthernet 0/25 | unassigned | NO  | Manual | up                    | down     |
| GigabitEthernet 0/26 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/27 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/28 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/29 | unassigned | NO  | Manual | administratively down | down     |
| GigabitEthernet 0/30 | unassigned | NO  | Manual | administratively down | down     |

## Interfaces > LAGS

### INTERFACES - LAGS

| Interface      | IP-Address | OK  | Method | Status | Protocol |
|----------------|------------|-----|--------|--------|----------|
| Port-channel 1 | unassigned | YES | Manual | up     | up       |
| Port-channel 2 | unassigned | YES | Manual | up     | up       |

## Interfaces > VLANs

### INTERFACES - VLANs

| Interface | IP-Address | OK  | Method | Status                | Protocol |
|-----------|------------|-----|--------|-----------------------|----------|
| Vlan 1    | unassigned | NO  | Manual | administratively down | down     |
| Vlan 2    | unassigned | NO  | Manual | administratively down | down     |
| Vlan 3    | unassigned | NO  | Manual | administratively down | down     |
| Vlan 4    | unassigned | NO  | Manual | administratively down | down     |
| Vlan 5    | unassigned | NO  | Manual | administratively down | down     |
| Vlan 1000 | 5.5.5.3    | YES | Manual | up                    | up       |
| Vlan 2000 | 16.16.16.2 | YES | Manual | up                    | up       |
| Vlan 2001 | 16.16.17.2 | YES | Manual | up                    | up       |
| Vlan 3000 | 24.24.24.3 | YES | Manual | up                    | up       |
| Vlan 3001 | unassigned | NO  | Manual | administratively down | down     |
| Vlan 3002 | unassigned | NO  | Manual | administratively down | down     |
| Vlan 3500 | unassigned | NO  | Manual | administratively down | down     |
| Vlan 4000 | unassigned | YES | Manual | up                    | up       |
| Vlan 4009 | unassigned | NO  | Manual | administratively down | down     |
| Vlan 4011 | unassigned | NO  | Manual | administratively down | down     |
| Vlan 4012 | unassigned | NO  | Manual | administratively down | down     |
| Vlan 4050 | 42.42.42.3 | YES | Manual | up                    | up       |

---

## Interfaces > Management

### INTERFACES - MANAGEMENT

| Interface          |      | IP-Address | OK  | Method | Status | Protocol    |
|--------------------|------|------------|-----|--------|--------|-------------|
| ManagementEthernet | 0/0  | 10.43.3.55 | YES | Manual | up     | up          |
| ManagementEthernet | 1/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 2/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 3/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 4/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 5/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 6/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 7/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 8/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 9/0  | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 10/0 | unassigned | NO  | Manual | up     | not present |
| ManagementEthernet | 11/0 | unassigned | NO  | Manual | up     | not present |

---

---

**Protocols Menu**

---

**Protocols > VRRP****PROTOCOLS - VRRP**

---

```

Vlan 100, IPv4 VRID: 1, Version: 2, Net: 88.1.1.1
State: Master, Priority: 101, Master: 88.1.1.1 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 2931984, Gratuitous ARP sent: 12
Virtual MAC address:
 00:00:5e:00:01:01
Virtual IP address:
 88.1.1.4 88.1.1.5 88.1.1.6 88.1.1.7
 88.1.1.8 88.1.1.9 88.1.1.10 88.1.1.11
 88.1.1.12 88.1.1.13 88.1.1.14 88.1.1.15
Authentication: (none)

```

```

Vlan 101, IPv4 VRID: 1, Version: 2, Net: 88.1.2.1
State: Master, Priority: 101, Master: 88.1.2.1 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 2930966, Gratuitous ARP sent: 12
Virtual MAC address:
 00:00:5e:00:01:01
Virtual IP address:
 88.1.2.4 88.1.2.5 88.1.2.6 88.1.2.7
 88.1.2.8 88.1.2.9 88.1.2.10 88.1.2.11
 88.1.2.12 88.1.2.13 88.1.2.14 88.1.2.15
Authentication: (none)

```

```

Vlan 102, IPv4 VRID: 1, Version: 2, Net: 88.1.3.1
State: Master, Priority: 101, Master: 88.1.3.1 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 2930214, Gratuitous ARP sent: 12
Virtual MAC address:
 00:00:5e:00:01:01
Virtual IP address:
 88.1.3.4 88.1.3.5 88.1.3.6 88.1.3.7
 88.1.3.8 88.1.3.9 88.1.3.10 88.1.3.11
 88.1.3.12 88.1.3.13 88.1.3.14 88.1.3.15
Authentication: (none)

```

```

Vlan 103, IPv4 VRID: 1, Version: 2, Net: 88.1.4.1
State: Master, Priority: 101, Master: 88.1.4.1 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 2929610, Gratuitous ARP sent: 12
Virtual MAC address:
 00:00:5e:00:01:01
Virtual IP address:
 88.1.4.4 88.1.4.5 88.1.4.6 88.1.4.7
 88.1.4.8 88.1.4.9 88.1.4.10 88.1.4.11
 88.1.4.12 88.1.4.13 88.1.4.14 88.1.4.15
Authentication: (none)

```

## Protocols > VRRP Brief

### PROTOCOLS - VRRP BRIEF

| Interface | Group  | Pri | Pre | State  | Master addr | Virtual addr(s)        | Description |
|-----------|--------|-----|-----|--------|-------------|------------------------|-------------|
| Vl 100    | IPv4 1 | 101 | Y   | Master | 88.1.1.1    | 88.1.1.4 88.1.1.5...   |             |
| Vl 101    | IPv4 1 | 101 | Y   | Master | 88.1.2.1    | 88.1.2.4 88.1.2.5...   |             |
| Vl 102    | IPv4 1 | 101 | Y   | Master | 88.1.3.1    | 88.1.3.4 88.1.3.5...   |             |
| Vl 103    | IPv4 1 | 101 | Y   | Master | 88.1.4.1    | 88.1.4.4 88.1.4.5...   |             |
| Vl 104    | IPv4 1 | 101 | Y   | Master | 88.1.5.1    | 88.1.5.4 88.1.5.5...   |             |
| Vl 105    | IPv4 1 | 101 | Y   | Master | 88.1.6.1    | 88.1.6.4 88.1.6.5...   |             |
| Vl 106    | IPv4 1 | 101 | Y   | Master | 88.1.7.1    | 88.1.7.4 88.1.7.5...   |             |
| Vl 107    | IPv4 1 | 101 | Y   | Master | 88.1.8.1    | 88.1.8.4 88.1.8.5...   |             |
| Vl 108    | IPv4 1 | 101 | Y   | Master | 88.1.9.1    | 88.1.9.4 88.1.9.5...   |             |
| Vl 109    | IPv4 1 | 101 | Y   | Master | 88.1.10.1   | 88.1.10.4 88.1.10.5... |             |
| Vl 110    | IPv4 1 | 101 | Y   | Master | 88.1.11.1   | 88.1.11.4 88.1.11.5... |             |
| Vl 111    | IPv4 1 | 101 | Y   | Master | 88.1.12.1   | 88.1.12.4 88.1.12.5... |             |
| Vl 112    | IPv4 1 | 101 | Y   | Master | 88.1.13.1   | 88.1.13.4 88.1.13.5... |             |
| Vl 113    | IPv4 1 | 101 | Y   | Master | 88.1.14.1   | 88.1.14.4 88.1.14.5... |             |
| Vl 114    | IPv4 1 | 101 | Y   | Master | 88.1.15.1   | 88.1.15.4 88.1.15.5... |             |
| Vl 115    | IPv4 1 | 101 | Y   | Master | 88.1.16.1   | 88.1.16.4 88.1.16.5... |             |
| Vl 116    | IPv4 1 | 101 | Y   | Master | 88.1.17.1   | 88.1.17.4 88.1.17.5... |             |
| Vl 117    | IPv4 1 | 101 | Y   | Master | 88.1.18.1   | 88.1.18.4 88.1.18.5... |             |
| Vl 118    | IPv4 1 | 101 | Y   | Master | 88.1.19.1   | 88.1.19.4 88.1.19.5... |             |
| Vl 119    | IPv4 1 | 101 | Y   | Master | 88.1.20.1   | 88.1.20.4 88.1.20.5... |             |
| Vl 120    | IPv4 1 | 101 | Y   | Master | 88.1.21.1   | 88.1.21.4 88.1.21.5... |             |
| Vl 121    | IPv4 1 | 101 | Y   | Master | 88.1.22.1   | 88.1.22.4 88.1.22.5... |             |
| Vl 122    | IPv4 1 | 101 | Y   | Master | 88.1.23.1   | 88.1.23.4 88.1.23.5... |             |
| Vl 123    | IPv4 1 | 101 | Y   | Master | 88.1.24.1   | 88.1.24.4 88.1.24.5... |             |
| Vl 124    | IPv4 1 | 101 | Y   | Master | 88.1.25.1   | 88.1.25.4 88.1.25.5... |             |
| Vl 125    | IPv4 1 | 101 | Y   | Master | 88.1.26.1   | 88.1.26.4 88.1.26.5... |             |
| Vl 126    | IPv4 1 | 101 | Y   | Master | 88.1.27.1   | 88.1.27.4 88.1.27.5... |             |
| Vl 127    | IPv4 1 | 101 | Y   | Master | 88.1.28.1   | 88.1.28.4 88.1.28.5... |             |
| Vl 128    | IPv4 1 | 101 | Y   | Master | 88.1.29.1   | 88.1.29.4 88.1.29.5... |             |
| Vl 129    | IPv4 1 | 101 | Y   | Master | 88.1.30.1   | 88.1.30.4 88.1.30.5... |             |
| Vl 130    | IPv4 1 | 101 | Y   | Master | 88.1.31.1   | 88.1.31.4 88.1.31.5... |             |
| Vl 131    | IPv4 1 | 101 | Y   | Master | 88.1.32.1   | 88.1.32.4 88.1.32.5... |             |
| Vl 132    | IPv4 1 | 101 | Y   | Master | 88.1.33.1   | 88.1.33.4 88.1.33.5... |             |
| Vl 133    | IPv4 1 | 101 | Y   | Master | 88.1.34.1   | 88.1.34.4 88.1.34.5... |             |
| Vl 134    | IPv4 1 | 101 | Y   | Master | 88.1.35.1   | 88.1.35.4 88.1.35.5... |             |
| Vl 135    | IPv4 1 | 101 | Y   | Master | 88.1.36.1   | 88.1.36.4 88.1.36.5... |             |
| Vl 136    | IPv4 1 | 101 | Y   | Master | 88.1.37.1   | 88.1.37.4 88.1.37.5... |             |
| Vl 137    | IPv4 1 | 101 | Y   | Master | 88.1.38.1   | 88.1.38.4 88.1.38.5... |             |
| Vl 138    | IPv4 1 | 101 | Y   | Master | 88.1.39.1   | 88.1.39.4 88.1.39.5... |             |
| Vl 139    | IPv4 1 | 101 | Y   | Master | 88.1.40.1   | 88.1.40.4 88.1.40.5... |             |
| Vl 140    | IPv4 1 | 101 | Y   | Master | 88.1.41.1   | 88.1.41.4 88.1.41.5... |             |
| Vl 141    | IPv4 1 | 101 | Y   | Master | 88.1.42.1   | 88.1.42.4 88.1.42.5... |             |
| Vl 142    | IPv4 1 | 101 | Y   | Master | 88.1.43.1   | 88.1.43.4 88.1.43.5... |             |
| Vl 143    | IPv4 1 | 101 | Y   | Master | 88.1.44.1   | 88.1.44.4 88.1.44.5... |             |
| Vl 144    | IPv4 1 | 101 | Y   | Master | 88.1.45.1   | 88.1.45.4 88.1.45.5... |             |
| Vl 145    | IPv4 1 | 101 | Y   | Master | 88.1.46.1   | 88.1.46.4 88.1.46.5... |             |
| Vl 146    | IPv4 1 | 101 | Y   | Master | 88.1.47.1   | 88.1.47.4 88.1.47.5... |             |

## Protocols > BGP Summary

### PROTOCOLS - BGP SUMMARY

BGP router identifier 222.222.222.222, local AS number 6338  
 BGP table version is 0, main routing table version 0  
 2 neighbor(s) using 12288 bytes of memory

| Neighbor   | AS   | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down | State/Pfx |
|------------|------|---------|---------|--------|-----|------|---------|-----------|
| 5.5.5.1    | 6338 | 10083   | 10070   | 0      | 0   | 0    | 1w0d    | 0         |
| 70.70.70.2 | 4383 | 0       | 0       | 0      | 0   | 0    | never   | Active    |

## Protocols > BGP Neighbors

### PROTOCOLS - BGP NEIGHBORS

```

BGP neighbor is 5.5.5.1, remote AS 6338, internal link
 BGP version 4, remote router ID 223.223.223.223
 BGP state ESTABLISHED, in this state for 1w0d
 Last read 00:00:41, last write 00:00:47
 Hold time is 180, keepalive interval is 60 seconds
 Received 10083 messages, 0 in queue
 1 opens, 0 notifications, 0 updates
 10082 keepalives, 0 route refresh requests
 Sent 10070 messages, 0 in queue
 1 opens, 0 notifications, 0 updates
 10069 keepalives, 0 route refresh requests
 Minimum time between advertisement runs is 5 seconds
 Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv4 Unicast :
 MULTIPROTO_EXT(1)
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv4 Unicast :
 MULTIPROTO_EXT(1)
 ROUTE_REFRESH(2)
 CISCO_ROUTE_REFRESH(128)

For address family: IPv4 Unicast
 BGP table version 0, neighbor version 0
 Prefixes accepted 0 (consume 0 bytes), withdrawn 0 by peer, martian prefixes ignored 0
 Prefixes advertised 0, denied 0, withdrawn 0 from peer

Connections established 1; dropped 0
 Last reset never
Local host: 5.5.5.3, Local port: 55170
Foreign host: 5.5.5.1, Foreign port: 179

```

## Protocols > OSPF Neighbors

### PROTOCOLS - OSPF NEIGHBORS

| Neighbor ID     | Pri | State   | Dead Time | Address    | Interface | Area |
|-----------------|-----|---------|-----------|------------|-----------|------|
| 223.223.223.223 | 1   | FULL/DR | 00:00:39  | 16.16.16.1 | Vl 2000   | 0    |
| 223.223.223.223 | 1   | FULL/DR | 00:00:33  | 16.16.17.1 | Vl 2001   | 0    |
| 223.223.223.223 | 1   | FULL/DR | 00:00:34  | 39.39.39.1 | Gi 0/39   | 0    |

## Protocols > ISIS Neighbors

### PROTOCOLS - ISIS NEIGHBORS

| System Id      | Interface | State     | Type     | Priority | Uptime      | Circuit Id                          |
|----------------|-----------|-----------|----------|----------|-------------|-------------------------------------|
| 0509.0001.0000 | Te 0/10   | Up/Up     | L1L2     | 0/0      | 2w5d/2w5d   | 0010.0100.1001.01/0010.0100.1001.01 |
| 0509.0002.0000 | Te 0/10   | Up        | L2       | 0        | 2w5d        | 0010.0100.1001.01                   |
| 0509.0003.0000 | Te 0/10   | Up        | L2       | 0        | 2w5d        | 0010.0100.1001.01                   |
| 0030.0300.3003 | Te 0/25   | Up/Up     | L1L2 (M) | 64/64    | 4w6d/4w6d   | 0010.0100.1001.02/0010.0100.1001.02 |
| 050C.0001.0000 | Te 0/46   | Up/Up     | L1L2     | 0/0      | 2w5d/2w5d   | 0010.0100.1001.04/0010.0100.1001.04 |
| 0020.0200.2002 | V1 100    | Init/Init | L1L2 (M) | 64/64    | 1d15h/1d4h  | 0020.0200.2002.06/0020.0200.2002.06 |
| 0030.0300.3003 | V1 100    | Init/Init | L1L2 (M) | 64/64    | 2w4d/2w4d   | 0020.0200.2002.06/0020.0200.2002.06 |
| 0030.0300.3003 | V1 101    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.07/0010.0100.1001.07 |
| 0030.0300.3003 | V1 102    | Up/Up     | L1L2 (M) | 64/64    | 1d10h/1d7h  | 0010.0100.1001.08/0010.0100.1001.08 |
| 0030.0300.3003 | V1 103    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.09/0010.0100.1001.09 |
| 0030.0300.3003 | V1 104    | Up/Up     | L1L2 (M) | 64/64    | 1d10h/1d10h | 0010.0100.1001.0A/0010.0100.1001.0A |
| 0030.0300.3003 | V1 105    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.0B/0010.0100.1001.0B |
| 0030.0300.3003 | V1 106    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d10h  | 0010.0100.1001.0C/0010.0100.1001.0C |
| 0030.0300.3003 | V1 107    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.0D/0010.0100.1001.0D |
| 0030.0300.3003 | V1 108    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.0E/0010.0100.1001.0E |
| 0030.0300.3003 | V1 109    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.0F/0010.0100.1001.0F |
| 0030.0300.3003 | V1 110    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.10/0010.0100.1001.10 |
| 0030.0300.3003 | V1 111    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.11/0010.0100.1001.11 |
| 0030.0300.3003 | V1 112    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.12/0010.0100.1001.12 |
| 0030.0300.3003 | V1 113    | Up/Up     | L1L2 (M) | 64/64    | 1d10h/1d10h | 0010.0100.1001.13/0010.0100.1001.13 |
| 0030.0300.3003 | V1 114    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.14/0010.0100.1001.14 |
| 0030.0300.3003 | V1 115    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.15/0010.0100.1001.15 |
| 0030.0300.3003 | V1 116    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d10h  | 0010.0100.1001.16/0010.0100.1001.16 |
| 0030.0300.3003 | V1 117    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.17/0010.0100.1001.17 |
| 0030.0300.3003 | V1 118    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.18/0010.0100.1001.18 |
| 0030.0300.3003 | V1 119    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.19/0010.0100.1001.19 |
| 0030.0300.3003 | V1 120    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.1A/0010.0100.1001.1A |
| 0030.0300.3003 | V1 121    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.1B/0010.0100.1001.1B |
| 0030.0300.3003 | V1 122    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.1C/0010.0100.1001.1C |
| 0030.0300.3003 | V1 123    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.1D/0010.0100.1001.1D |
| 0030.0300.3003 | V1 124    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.1E/0010.0100.1001.1E |
| 0030.0300.3003 | V1 125    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.1F/0010.0100.1001.1F |
| 0030.0300.3003 | V1 126    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.20/0010.0100.1001.20 |
| 0030.0300.3003 | V1 127    | Up/Up     | L1L2 (M) | 64/64    | 1d15h/1d7h  | 0010.0100.1001.21/0010.0100.1001.21 |
| 0030.0300.3003 | V1 128    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.22/0010.0100.1001.22 |
| 0030.0300.3003 | V1 129    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.23/0010.0100.1001.23 |
| 0030.0300.3003 | V1 130    | Up/Up     | L1L2 (M) | 64/64    | 1d7h/1d7h   | 0010.0100.1001.24/0010.0100.1001.24 |

## Diagnostics Menu

## Diagnostics &gt; Arp Table

## ARP TABLE

| Protocol | Address      | Age(min) | Hardware Address  | Interface | VLAN    | CPU |
|----------|--------------|----------|-------------------|-----------|---------|-----|
| Internet | 5.5.5.1      | 87       | 00:01:e8:8c:44:aa | Gi 0/3    | Vl 1000 | CP  |
| Internet | 5.5.5.3      | -        | 00:01:e8:9b:00:02 | -         | Vl 1000 | CP  |
| Internet | 10.43.0.1    | 0        | 00:06:28:5d:4f:c2 | Ma 0/0    | -       | CP  |
| Internet | 10.43.254.20 | 7        | 00:0c:29:2a:6e:cc | Ma 0/0    | -       | CP  |
| Internet | 16.16.16.1   | 71       | 00:01:e8:8c:44:aa | Gi 0/14   | Vl 2000 | CP  |
| Internet | 16.16.16.2   | -        | 00:01:e8:9b:00:02 | -         | Vl 2000 | CP  |
| Internet | 16.16.17.1   | 71       | 00:01:e8:8c:44:aa | Po 1      | Vl 2001 | CP  |
| Internet | 16.16.17.2   | -        | 00:01:e8:9b:00:02 | -         | Vl 2001 | CP  |
| Internet | 24.24.24.3   | -        | 00:01:e8:9b:00:02 | -         | Vl 3000 | CP  |
| Internet | 39.39.39.1   | 71       | 00:01:e8:8c:44:aa | Gi 0/39   | -       | CP  |
| Internet | 39.39.39.2   | -        | 00:01:e8:9b:00:02 | Gi 0/39   | -       | CP  |
| Internet | 42.42.42.3   | -        | 00:01:e8:9b:00:02 | -         | Vl 4050 | CP  |

## Diagnostics &gt; Mac Address Table

## MAC ADDRESS TABLE

| VlanId | Mac Address       | Type    | Interface | State  |
|--------|-------------------|---------|-----------|--------|
| 1000   | 00:01:e8:8c:44:aa | Dynamic | Gi 0/3    | Active |
| 2000   | 00:01:e8:8c:44:aa | Dynamic | Gi 0/14   | Active |
| 2001   | 00:01:e8:8c:44:aa | Dynamic | Po 2      | Active |

## Diagnostics &gt; Routing Table

## ROUTING TABLE

Codes: C - connected, S - static, R - RIP,  
 B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated,  
 O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,  
 N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,  
 E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,  
 L2 - IS-IS level-2, IA - IS-IS inter area, \* - candidate default,  
 > - non-active route, + - summary route

Gateway of last resort is not set

|   | Destination        | Gateway         | Dist/Metric | Last Change |
|---|--------------------|-----------------|-------------|-------------|
| C | 5.5.5.0/24         | Direct, Vl 1000 | 0/0         | 1w0d        |
| C | 16.16.16.0/24      | Direct, Vl 2000 | 0/0         | 1w0d        |
| C | 16.16.17.0/24      | Direct, Vl 2001 | 0/0         | 1w0d        |
| C | 24.24.24.0/24      | Direct, Vl 3000 | 0/0         | 1w0d        |
| C | 39.39.39.0/24      | Direct, Gi 0/39 | 0/0         | 1w0d        |
| C | 42.42.42.0/24      | Direct, Vl 4050 | 0/0         | 1w0d        |
| C | 222.222.222.222/32 | Direct, Lo 0    | 0/0         | 1w0d        |



## Diagnostics > System Log

### SYSTEM LOG

```
Syslog logging: enabled
 Console logging: level debugging
 Monitor logging: level debugging
 Buffer logging: level debugging, 234 Messages Logged, Size (40960 bytes)
 Trap logging: level informational
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGOUT: Exec session is terminated for user admin on line vty0 (10.43.254.20)
1w0d1h: %STKUNITO-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password authentication success on vty0 (10.4
1w0d1h: %STKUNITO-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for user admin on vty0 (10.43.254.20)
```

## Diagnostics &gt; VLANs

## VLANs

Codes: \* - Default VLAN, G - GVRP VLANs, P - Primary, C - Community, I - Isolated  
 Q: U - Untagged, T - Tagged  
 x - Dot1x untagged, X - Dot1x tagged  
 G - GVRP tagged, M - Vlan-stack, H - VSN tagged

| NUM  | Status   | Description | Q Ports                                |
|------|----------|-------------|----------------------------------------|
| * 1  | Inactive |             | U Gi 0/25,47                           |
| 2    | Inactive |             |                                        |
| 3    | Inactive |             |                                        |
| 4    | Inactive |             |                                        |
| 5    | Inactive |             |                                        |
| 1000 | Active   |             | T Gi 0/3                               |
| 2000 | Active   | OSPF        | T Gi 0/14                              |
| 2001 | Active   |             | T Po1(Gi 0/21-23)<br>T Po2(Gi 0/10-12) |
| 3000 | Active   | ISIS        | T Gi 0/3                               |
| 3001 | Inactive |             |                                        |
| 3002 | Inactive |             |                                        |
| 3500 | Active   | L2          | T Gi 0/37                              |
| 4000 | Active   | L2          | T Gi 0/42                              |
| 4009 | Inactive |             |                                        |
| 4011 | Inactive |             |                                        |
| 4012 | Inactive |             |                                        |
| 4050 | Active   | L3          | T Gi 0/20                              |

## Diagnostics &gt; VLAN Members

## VLAN MEMBERS

Select VLAN ID .....

## SELECTED VLAN

Codes: \* - Default VLAN, G - GVRP VLANs, P - Primary, C - Community, I - Isolated  
 Q: U - Untagged, T - Tagged  
 x - Dot1x untagged, X - Dot1x tagged  
 G - GVRP tagged, M - Vlan-stack, H - VSN tagged

| NUM  | Status | Description | Q Ports                                |
|------|--------|-------------|----------------------------------------|
| 2001 | Active |             | T Po1(Gi 0/21-23)<br>T Po2(Gi 0/10-12) |

---

## Diagnostics > Int Bandwidth

### BANDWIDTH

---

Enter Stack Unit .....   
Enter Port .....

### BANDWIDTH DATA

---

```
Rate info (interval 299 seconds):
 Input 00.00 Mbits/sec, 1 packets/sec, 0.00% of line-rate
 Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 1w0d1h
```

---

**Utilities Menu**

---

**Utilities > Ping****PING**Enter IP Address (No Hostnames) ..... **PING DATA**

```
Sending 5, 100-byte ICMP Echos to 10.42.0.13, timeout is 2 seconds:
!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max = 0/0/0 (ms)
```

---

**Utilities > Traceroute****TRACE**Enter IP Address (No Hostnames) ..... Enter Timeout ..... **TRACE DATA**

```

Tracing the route to 10.42.0.13, 30 hops max, 40 byte packets

```

| TTL | Hostname   | Probe1     | Probe2     | Probe3     |
|-----|------------|------------|------------|------------|
| 1   | 10.43.0.1  | 000.000 ms | 000.000 ms | 000.000 ms |
| 2   | 10.42.0.13 | 000.000 ms | 006.000 ms | 000.000 ms |

---

## Settings Menu

---

### Settings > SmartUtils Credentials

#### SMARTUTILS USER CREDENTIALS

---



This username and password must exist on FTOS and have privilege level 15 or enable password.

#### Configure credentials used by SmartUtils to communicate with FTOS

---

Enter User Name .....

Enter Password .....

Enter Enable Password .....

