Contents

Chapter 1

FTOS Quick Start ......................................................... 3

Introduction ............................................................. 3
FTOS CLI ................................................................. 4
Logging in for the first time ........................................... 4
Access the Command Line ............................................. 5
Access the C-Series and E-Series remotely ....................... 5
Access the S-Series remotely ....................................... 5
Configure the Enable password .................................... 6
Enable a physical interface .......................................... 6
Configure interface for Layer 2 .................................... 6
Configure interface for Layer 3 (add an IP address) .......... 6
Change default VLAN .................................................. 7
Create new VLANs ..................................................... 7
Create Port Channels (LAGs) ....................................... 7
Add a physical interface to a port channel ..................... 8
Configure the minimum oper up links in a port channel (LAG) .................................................. 8
Add a port channel to a VLAN ..................................... 8
Configure LACP for dynamic port-channels ................. 8
Configure PoE ............................................................ 9
Set PoE power inline priority .................................... 9
Configure STP, MSTP, PVST+ or RSTP ..................... 9
Configure MSTP instances ....................................... 9
Add an interface to a spanning tree group .................. 10
Set up Network Time Protocol (NTP) ......................... 10
Configure FTOS system times .................................. 10

Chapter 2

Technical Support .......................................................... 11

The iSupport Website ................................................. 11
Accessing iSupport Services ...................................... 11
Contacting the Technical Assistance Center ............... 12
Requesting a Hardware Replacement ......................... 13
Chapter 1  FTOS Quick Start

Introduction

This document is intended to guide you through the CLIs to get your system up and running. More detailed procedures, including sample output configurations, are available in the FTOS Command Line Reference Guide and the FTOS Configuration Guide.

A version of FTOS is pre-loaded onto the chassis, however the system is not configured when you power up for the first time, except for the default hostname (Force10). You must configure the system initially using the Command Line Interface (CLI).

Refer to the Installation Guide for your platform for detailed instructions regarding the cabling and pin-outs for connections. This document assumes some system knowledge, including the location of your console port. If you do not, contact Force10 Networks’ Technical Support.

The information contained in this chapter instructs you regarding the following:

General Info
- FTOS CLI organization and use

First Things First
- Logging in for the first time
- Access the Command Line
  - Access the C-Series and E-Series remotely
  - Access the S-Series remotely
- Configure the Enable password

Interfaces
- Enable a physical interface
- Configure interface for Layer 2
- Configure interface for Layer 3 (add an IP address)
- Change default VLAN
- Create new VLANs
- Create Port Channels (LAGs)
- Add a physical interface to a port channel
- Add a port channel to a VLAN
- Configure LACP for dynamic port-channels

Power over Ethernet
- Configure PoE
- Set PoE power inline priority

Spanning Tree protocols
- Configure STP, MSTP, PVST+ or RSTP
- Configure MSTP instances
- Add an interface to a spanning tree group

System Calendar
- Set up Network Time Protocol (NTP)
- Configure FTOS system times
FTOS CLI

The FTOS CLI is divided into three major mode levels:

• **EXEC mode** is the default mode and has a privilege level of 1, which is the most restricted level. Only a limited selection of commands is available, notably *show* commands, which allow you to view system information.

• **EXEC Privilege mode** has commands to view configurations, clear counters, manage configuration files, run diagnostics, and enable or disable debug operations. The privilege level is 15, which is unrestricted. You can configure a password for this mode.

• **CONFIGURATION mode** enables you to configure security features, time settings, set logging and SNMP functions, configure static ARP and MAC addresses, and set line cards on the system. Beneath CONFIGURATION mode are sub-modes that apply to interfaces, protocols, and features. Two sub-CONFIGURATION modes are important when configuring the chassis for the first time:

  • **INTERFACE sub-mode** is the mode in which you configure Layer 2 and Layer 3 protocols and IP services specific to an interface. An interface can be physical (Management interface, 1-Gigabit Ethernet, or 10-Gigabit Ethernet, or SONET) or logical (Loopback, Null, port channel, or VLAN).

  • **LINE sub-mode** is the mode in which you configure the console and virtual terminal lines.

  **Note:** At any time, entering a question mark (?) will display the available command options. For example, when you are in CONFIGURATION mode, entering the question mark first will list all available commands, including the possible sub-modes.

  **Note:** At any time, preceding a command with *no*, removes the command from the configuration and returned to the default. For example, *no ip address* removes the IP address from an interface.

**Logging in for the first time**

1. Enter your Login user ID and password.
   - This is the Exec mode (Force10>). In this mode you can view some but not all commands.

2. While in EXEC mode, enter command *enable* and hit the enter button. This may prompt you for a password; the default is no password so hit enter again.
   - This is EXEC Privilege mode (Force10#). In this mode you can view more commands and perform some configuration changes.

3. While in EXEC Privilege mode, type the command *configuration* and hit enter.
   - This is CONFIGURATION mode (Force10(config)#). In this mode, you can configure your system and enter other specific sub-modes (Interface, VLAN, etc).

4. Enter *exit* at any prompt to return to the previous mode.
Access the Command Line

Access the command line initially through the serial console port. When the system successfully boots, you enter the command line in the EXEC mode. In order to log in to the system remotely (Telnet or SSH) you must set up a user name and password.

Access the C-Series and E-Series remotely

Configuring the system for Telnet is a three-step process:

1. Configure an IP address for the management port.
   
   Force10(config)#interface ManagementEthernet slot/port
   Force10(conf-if-ma-0/0)#ip address ip-address/mask
   Force10(conf-if-ma-0/0)#no shutdown

2. Configure a management route with a default gateway.
   
   Force10(config)#management route ip-address/mask gateway

3. Configure a username and password.
   
   Force10(config)#username username password [encryption-type] password

4. Configure static routes.
   
   Force10(config)#ip route ip-address mask [ip-address | interface [ip-address]] [distance] [permanent] [tag tag-value]
   or
   
   Force10(config)#ipv6 route ipv6-address prefix-length [ipv6-address | interface | interface ipv6-address] [distance] [tag value] [permanent]

Access the S-Series remotely

The S-Series does not have a dedicated management port nor a separate management routing table. Configure any port on the S-Series to be the port through which you manage the system and configure an IP route to that gateway.

1. Enter the CONFIGURATION mode.
   
   Force10#config

2. Configure an IP address for the port through which you will manage the system.
   
   Force10(config-if-gi-0/1)#ip address ip-address/mask

3. Configure a IP route with a default gateway.
   
   Force10#ip route ip-address mask {ip-address | interface [ip-address]} [distance] [permanent] [tag tag-value]

4. Configure a username and password.
   
   Force10# username username password [encryption-type] password
Configure the Enable password

Access the EXEC Privilege mode using the `enable` command. The EXEC Privilege mode is unrestricted by default. Configure a password as a basic security measure. There are two types of `enable` passwords:

- `enable password` stores the password in the running/startup configuration using a DES encryption method.
- `enable secret` stores the password in the running/startup configuration using an MD5 encryption method.

1. While you are in CONFIGURATION mode, create the enable password.
   ```
   Force10 (config)# enable [password | secret] [level level] [encryption-type] password
   ```

Enable a physical interface

1. From CONFIGURATION mode, enter INTERFACES mode.
   ```
   Force10 (config)# interface interface-type
   or
   Force10 (config)# interface interface-range
   ```
2. Enter the `no shutdown` command to enable the interface.
   ```
   Force10 (conf-if-gi-0/1)# no shutdown
   ```
3. Enter a description for the interface, if desired.
   ```
   Force10 (conf-if-gi-0/1)# description string
   ```

Configure interface for Layer 2

1. From INTERFACE mode, be sure the interface is enabled.
   ```
   Force10 (conf-if-gi-0/1)# no shutdown
   ```
2. Put the interface into Layer 2 mode.
   ```
   Force10 (conf-if-gi-0/1)# switchport
   ```

Configure interface for Layer 3 (add an IP address)

1. From INTERFACE mode, be sure the interface is enabled.
   ```
   Force10 (conf-if-gi-0/1)# no shutdown
   ```
2. Put the interface into Layer 3 mode.
   ```
   Force10 (conf-if-gi-0/1)# ip address address/mask
   ```
Change default VLAN

When interfaces are configured for Layer 2 mode, they are automatically placed in the Default VLAN as untagged interfaces. Only untagged interfaces can belong to the Default VLAN.

By default, VLAN 1 is the Default VLAN. To change that designation, use the `default vlan-id` command in the `CONFIGURATION` mode. You cannot delete the Default VLAN.

1. From `CONFIGURATION` mode, change the Default VLAN ID.

   `Force10(conf)#default vlan-id vlan-id`

Create new VLANs

1. From `CONFIGURATION` mode, create a new VLAN enter the `INTERFACE VLAN` mode.

   `Force10(conf)#interface vlan vlan-id`

2. Enter a description for the VLAN, if desired.

   `Force10(conf-if-vl-10)#description string`

3. Add a tagged port to the VLAN.

   `Force10(conf-if-vl-10)#tagged interface interface`

4. Add an untagged port to the VLAN.

   `Force10(conf-if-vl-10)#untagged interface interface`

5. Assign an IP address to the VLAN.

   `Force10(conf-if-vl-10)#ip address address/mask`

6. Enable the VLAN.

   `Force10(conf-if-vl-10)#no shutdown`

Create Port Channels (LAGs)

FTOS supports two types of port channels. This section discusses creating static port channels. Go to the LACP section for the steps to Configure LACP for dynamic port-channels.

1. From `CONFIGURATION` mode, create a new port channel and enter the `INTERFACE Port channel` mode.

   `Force10(conf)#interface port-channel port-channel number`

2. Enter a description for the port channel, if desired.

   `Force10(conf-if-po-10)#description string`
3. Configure the port-channel for Layer 2 or Layer 3 mode.

    Force10(conf-if-po-10)#switchport
    or
    Force10(conf-if-po-10)#ip address address/mask

Add a physical interface to a port channel

- From INTERFACE port channel mode, enter the channel member.

    Force10(conf-if-po-10)#channel-member interface

Configure the minimum oper up links in a port channel (LAG)

- From INTERFACE port channel mode, enter the channel member.

    Force10(conf-if-po-10)#minimum-links number

Add a port channel to a VLAN

As with other interfaces, you can add Layer 2 port channel interfaces to VLANs. To add a port channel to a VLAN, you must place the port channel in Layer 2 mode (by using the switchport command).

1. From INTERFACE port channel mode, add a tagged port channel to the VLAN.

    Force10(conf-if-vl-10)#tagged port-channel member number

2. From INTERFACE port channel mode, add an untagged port-channel to the VLAN.

    Force10(conf-if-vl-10)#untagged port-channel member number

Configure LACP for dynamic port-channels

1. Create Port Channels (LAGs).

2. From INTERFACE mode, enter the channel member.

    Force10(conf-if-gi-0/1)#port-channel-protocol lacp

3. Place the port-channel in active LACP mode.

    Force10(conf-if-gi-0/1)#port-channel number mode active
Configure PoE

Supporting PoE requires that the IEEE 802.3af-compliant powered device is directly connected to a port.

1. From CONFIGURATION mode, enter INTERFACES mode for the connected port.
   Force10(config)#interface interface-type
2. Enable PoE on the connected port.
   Force10(conf-if-gi-0/1)#power inline auto|static

Set PoE power inline priority

- While in INTERFACE mode, configure the connected port’s priority.
  Force10(config)#power inline priority Critical|high|low

Configure STP, MSTP, PVST+ or RSTP

1. While in INTERFACE mode, set the interface to Layer 2 mode.
   Force10(conf-if-gi-0/1)#no ip address
   Force10(conf-if-gi-0/1)#switchport
   Force10(conf-if-gi-0/1)#no shutdown
2. Return to CONFIGURATION mode, then enter INTERFACE VLAN Mode to assign interfaces to a VLAN.
   Force10(conf-if-gi-0/1)#exit
   Force10(config)# interfaces vlan 10
   Force10(config-if-vl-10)#tagged interface interface
   or
   Force10(config-if-vl-10)#tagged interface interface
3. Return to CONFIGURATION mode, then enter PVST Mode to configure PVST+ globally.
   Force10(conf-if-vl-10)#exit
   Force10(config)#protocol spanning-tree 0|mstp|pvst|rstp
   Force10(conf-pvst)#no disable

Configure MSTP instances

1. While in INTERFACES MSTP mode, assign MSTP instances.
   Force10(conf-mstp)#msti instance number vlan vlan-id
Add an interface to a spanning tree group

- While in INTERFACE mode, assign it to the Spanning Tree group.
  Force10(conf-if-gi-0/1)#spanning-tree 0
  or
  Force10(conf-if-gi-0/1)#spanning-tree mstp
  or
  Force10(conf-if-gi-0/1)#spanning-tree pvst
  or
  Force10(conf-if-gi-0/1)#spanning-tree rstp

Set up Network Time Protocol (NTP)

1. In CONFIGURATION mode, specify the NTP server.
   Force10(config)#ntp server ip-address
2. Set the hardware clock updates to come from NTP.
   Force10(config)#ntp update-calendar period
3. Enter INTERFACE mode and configure the interfaces as the broadcast client.
   Force10(conf-if-gi-0/1)#ntp broadcast client

Configure FTOS system times

1. In EXEC Privilege mode, set the time and date for the system hardware clock.
   Force10#calendar set time month day year
2. Set the time and date for the system software clock.
   Force10#clock set time month day year
3. Set the timezone.
   Force10#clock timezone timezone-name offset
4. Set daylight savings time once.
   Force10#clock summer-time time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]
5. Set daylight savings time as recurring update.
   Force10#clock summer-time time-zone recurring start-month start-day start-year start-time end-month end-day end-year end-time [offset]
This appendix contains these major sections:

- **The iSupport Website**
- **Contacting the Technical Assistance Center on page 12**
- **Requesting a Hardware Replacement on page 13**

## The iSupport Website

iSupport provides a range of documents and tools to assist you with effectively using Force10 equipment and mitigating the impact of network outages. Through iSupport you can obtain technical information regarding Force10 products, access to software upgrades and patches, and open and manage your Technical Assistance Center (TAC) cases. Force10 iSupport provides integrated, secure access to these services.

The i-Support website (http://www.force10networks.com/support/) contains a publicly available interface that includes access to techtips, white papers, and user manuals. After you get an account and log in, the available documentation expands to other types, including bug lists, error message decoder, release notes. You can even track your own Force10 inventory.

Once you are logged in, the following five tabs become available:

- **Home:** Summary of open cases, RMA management, and field notices (as shown below)
- **Service Request:** Case management
- **Software Center:** Software downloads, bug fixes, and bug tracking tool
- **Documents:** User documentation, FAQs, field notices, technical tips, and white papers
- **Support Programs:** Information on the suite of Force10 support and professional support services.

The Support Policies section of iSupport contains the *Support Guide*, which details the types of information and services that you can access through iSupport and through various types of support contracts.

## Accessing iSupport Services

The URL for iSupport is http://www.force10networks.com/support/. To access iSupport services you must have a userid and password. If you do not have one, you can request one at the website:
1. On the Force10 Networks iSupport page, click the Account Request link.

2. Fill out the User Account Request form, and click Send. You will receive your userid and password by E-mail.

3. To access iSupport services, click the LOGIN link, and enter your userid and password. See Contacting the Technical Assistance Center, below, for more.

### Contacting the Technical Assistance Center

|----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Information to Submit When Opening a Support Case | • Your name, company name, phone number, and E-mail address  
• Preferred method of contact  
• Model number  
• Serial Number (see Requesting a Hardware Replacement on page 13)  
• Software version number  
• Symptom description  
• Screen shots illustrating the symptom, including any error messages. These can include:  
  • Output from the `show tech-support [non-paged]` command (This report is very long, so the storage buffer in your terminal program should be set high.)  
  • Output from the `show logging eventlog [unit]` command, where `unit` is the stack ID of the member unit that experienced the failure (This report is included as a section in the output of `show tech-support`.)  
  • Console captures showing the error messages  
  • Console captures showing the troubleshooting steps taken  
  • Saved messages to a syslog server, if one is used |
| Managing Your Case | Log in to iSupport, and select the Service Request tab to view all open cases and RMAs. |
| Downloading Software Updates | Log in to iSupport, and select the Software Center tab. |
| Technical Documentation | Log in to iSupport, and select the Documents tab. This page can be accessed without logging in via the Documentation link on the iSupport page. |
| Contact Information | E-mail: support@force10networks.com  
Telephone:  
  US and Canada: 866.965.5800  
  International: 408.965.5800 |
Requesting a Hardware Replacement

To request replacement hardware, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Determine the part number and serial number of the component. To list the numbers for all components installed in the chassis, use the <strong>show hardware</strong> command.</td>
</tr>
</tbody>
</table>
| 2    | Request a Return Materials Authorization (RMA) number from TAC by opening a support case. Open a support case by:  
  - Using the Create Service Request form on the iSupport page (see **Contacting the Technical Assistance Center on page 12**).  
  - Contacting Force10 directly by E-mail or by phone (see **Contacting the Technical Assistance Center on page 12**). Provide the following information when using E-mail or phone:  
    - Part number, description, and serial number of the component.  
    - Your name, organization name, telephone number, fax number, and e-mail address.  
    - Shipping address for the replacement component, including a contact name, phone number, and e-mail address.  
    - A description of the failure, including log messages. This generally includes:  
      - Output from the **show tech-support [non-paged]** command (This report is very long, so the storage buffer in your terminal program should be set high.)  
      - Output from the **show logging eventlog [unit]** command, where *unit* is the stack ID of the member unit that experienced the failure (This report is included as a section in the output of **show tech-support**.)  
      - Console captures showing the error messages  
      - Console captures showing the troubleshooting steps taken  
      - Saved messages to a syslog server, if one is used |