S-Series and FTOS Release Notes

FTOS Version 7.8.1.0 **December 4, 2008**

Part Number: 101-00339-00

Table of Contents

For more information on hardware and software features, commands, and capabilities, refer to the documents on the Technical Publication CD-ROM or visit Force10 Networks, Inc. on the Web at www.force10networks.com.

How To Use This Document

This document contains information on open and resolved caveats, and operational information specific to the Force10 OS (FTOS™) software. Force10 Networks® platforms supported by FTOS 7.8.1 are the C-Series, E-Series®, and some S-Series models, as detailed in their respective release notes.

Caveats are unexpected or incorrect behavior, and are listed in order of Problem Report (PR) number within the appropriate sections.

Note: Customers can subscribe to caveat update reports or use the BugTrack search tool to read current information about open and closed software caveats. To subscribe or use BugTrack, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx. BugTrack currently tracks software caveats opened in FTOS version 6.2.1.1 and later.

All Release Notes are available on the Software Center tab of iSupport. The link to the relevant Release Notes for each software version is next to the link for that version:

https://www.force10networks.com/CSPortal20/Software/Downloads.aspx

New Hardware Features

10/100Base-T Copper SFP Support on the S25P: The S-Series S25P model now supports 10/100/1000Base-T on copper SFPs (catalog #GP-SFP2-1T). Previous versions of FTOS supported 1000Base-T on the S25P.

Supported Hardware

Hardware	Catalog Number	Minimum Software Version Required
S25P	S25-01-GE-24P-AC	7.6.1.0
S25P-DC	S25-01-GE-24P-DC	7.6.1.0
S25N	S25-01-GE-24T	7.7.1.0
S25V	S25-01-GE-24V	7.7.1.0
S50N	S50-01-GE-48T-AC	7.6.1.0
S50N-DC	S50-01-GE-48T-DC	7.6.1.0
S50V	S50-01-GE-48T-V	7.6.1.0

Default CLI Syntax or Behavior Changes

System

- **Visual Indication of Master, Standby, Member Status**: FTOS 7.7.1.1 introduces the Stacking Indicator LED on the face of the switch now displays an “A” to the left of the unit number if the unit is the stack master (including standalone unit), a “B” if the switch is the backup unit (standby master), or a “0” if it is a non-management stack member.
- FTOS 7.8.1.0 changes the output of the **show system brief** command output slightly, changing "Mgmt" to "Management", as shown below:

Figure 1   show system brief Command Output

```
Force10#show system  brief

Stack MAC : 00:01:e8:59:23:45

--  Stack Info  --
Unit  UnitType     Status         ReqTyp      CurTyp      Version     Ports
---------------------------------------------------------------------------
  0   Standby      online         S25V        S25V        7.8.1.0     28
  1   Member       online         S25P        S25P        7.8.1.0     28
  2   Management   online         S25N        S25N        7.8.1.0     28
  3   Member       not present
  4   Member       not present
  5   Member       not present
  6   Member       not present
  7   Member       not present
```

Protocols

AAA Authentication Timeouts — The timeout behavior in FTOS 7.8.1.0 is changed to:

- Timeout between servers = 10 seconds (by default and user configurable)
- Timeout between methods = 40 seconds

The timeout before FTOS 7.8.1.0 is the same 10 seconds between servers, but also 10 seconds between methods.

LLDP — FTOS 7.7.1.1 adds the remote system name to the **show lldp neighbor** report output. To show the system name to the LLDP neighbors, the systems must advertise their system name.

Note: LLDP neighbors of a system running versions of FTOS prior to 7.7.1.1 display the chassis ID (for example, 00:01:e8:0d:b6:d6) in place of the hostname.

Power over Ethernet (PoE) — FTOS 7.7.1.1 and later supports the **no power inline** command to disable PoE.

FTOS 7.8.1.0 Software Features

The table briefly describes the new software features introduced in FTOS version 7.8.1.0 for the S-Series.

Table 2: New Software Features for the S-Series

"ignore-case" Option for the grep CLI Command: The **`grep`** CLI command to search for a pattern in CLI output is extended with the ignore-case option to ignore case distinctions.
10/100Base-T Copper SFP Support on the S25P: The S-Series S25P now supports 10/100/1000Base-T on copper SFPs (catalog # GP-SFP2-1T). Previous versions of FTOS supported 1000Base-T on the S25P.
CPU and Memory Utilization SNMP OIDs for Stack Units: The S-Series manageability feature set is extended with SNMP OIDs in the FORCE10-SS-CHASSIS-MIB to poll the CPU and memory utilization on stack units. FTOS 7.7.1.0 supported OIDs for standalone and stack master units.
Digital Optical Monitoring (DOM) on Qualified Force10 SFP and SFP+ Optical Media Modules: The FTOS serviceability feature set is enhanced to support Digital Optical Monitoring (DOM) on qualified Force10 SFP and SFP+ optical media modules. DOM enables users to view real-time media module parameters for monitoring and troubleshooting. The **`show interfaces transceiver`** output is augmented with diagnostic fields.
Enhanced Stack Reset Log Messages: The FTOS stacking feature is extended with more descriptive log messages when a stack unit is reset.
Ethernet Flow Control: IEEE 802.3x pause frames are a control frame that can be used to throttle input on an interface if a device is overwhelmed by traffic. The interface CLI command flowcontrol to enable pause frames is now supported on the C-Series and S-Series switch/routers. Pause frames were ignored in previous versions of FTOS on these platforms. This feature was also introduced in FTOS 7.7.1.1.
Format the Flash Filesystem: The FTOS CLI command to format the flash: file system is now available on S-Series standalone, stack master and standby units. This feature is also available in FTOS 7.7.1.1.
Hardware Serviceability and Diagnostic CLI Commands: The FTOS serviceability feature set for hardware diagnostics and debugging is extended to the S-Series. CLI commands to display and clear forwarding path and ASIC statistics for troubleshooting hardware problems are now available to debug potential hardware problems. This feature is also available in FTOS 7.7.1.1.
IGMPv1/v2 Snooping on Stack Units: FTOS 7.6.1.0 introduced IGMPv1/v2 snooping on S-Series standalone and stack master units. In FTOS 7.8.1.0, IGMPv1/v2 snooping is now also supported on stack member units.
IP Multicast Policies: The FTOS IP multicast policy feature set is extended to the C-Series and S-Series. These platforms now support policies to limit the number of groups, neighbors, and multicast routes.
IPv6 Routing: The FTOS IPv6 routing feature set is extended to S-Series switch/routers with IPv6 addressing, static routing, and management features.
Longer Names for ACLs and Routing Policies: FTOS now allows names of ACLs, policy maps, and route maps to be up to 140 characters long. FTOS versions prior to 7.8.1.0 supported a maximum length of 16 characters.
Multiple Tagging Support on VLAN Stacking Trunk Ports: The FTOS VLAN stacking implementation on the C-Series and S-Series now supports forwarding of VLAN stack and 802.1Q VLAN frames on the same port, allowing users greater flexibility when deploying VLAN stacking.
Multi-process OSPF: Multi-process OSPF provides an option for creating multiple OSPF processes on a single router with separate databases. This feature can be used to virtualize a physical topology into logical routing domains, which can each support different routing and security policies. FTOS supports 28 processes on the E-Series, six processes on the C-Series, and three processes on the S-Series.
Network Boot Option: The S-Series manageability feature set is enhanced to support booting over the network using TFTP, to allow users more flexibility in managing software images and versions on standalone units.
New Password Recovery Mechanism: The S-Series password recovery mechanism is changed to function more similarly to the way it does on the E-Series and C-Series.

Table 2: New Software Features for the S-Series (continued)

Offline Diagnostics on Stacking Units: Offline diagnostics extend the FTOS serviceability feature set for diagnostics and debugging on S-Series stack units. Diagnostics are started and monitored from the FTOS CLI. Test results, including detailed statistics for all tests, are then displayed via the CLI. FTOS 7.7.1.0 introduced offline diagnostics on standalone and stack master units. The S-Series Debug chapter contains several more versions of the show hardware command, along with associated versions of the clear hardware command, all introduced in FTOS 7.7.1.1.
OSPF Fast Convergence: The FTOS OSPF implementation is optimized further to improve convergence time, and also features new commands that can be used to control LSA origination and processing.
OSPF Graceful Restart: The full FTOS OSPF graceful restart functionality, as defined in RFC 3623, is now available on the S-Series. Previous versions of FTOS supported helper mode.
Port-Based Rate Policing on Layer 3 Interfaces: The FTOS QoS features set on the C-Series and S-Series is extended to support port-based rate policing on Layer 3 interfaces. Previous versions of FTOS supported this feature on Layer 2 interfaces.
Private VLAN: Private VLANs (PVLANs) extend the FTOS security suite by virtualizing a shared VLAN into subdomains identified by a primary and secondary VLAN pair. Each primary VLAN supports multiple secondary community or isolated VLANs. Devices on community VLANs can communicate with each other via member ports, while devices on isolated VLANs cannot. The FTOS private VLAN implementation is based on RFC 3069.
Programmable (S,G) Expiry Timer: By default, all PIM-SM (S,G) entries expire in 210 seconds. For some multicast applications it is desirable that certain (S,G) pairs be retained for an extended period of time, even in the absence of an active source. The command **ip pim sparse-mode sg-expiry-timer** is added to configure the expiry time globally for all sources, or for a specific set of (S,G) pairs defined by an access list. This feature was also introduced in FTOS 7.7.1.1.
QoS Policy Scalability Optimizations: The QoS policy manager is optimized to use hardware tables more efficiently. A single copy of each policy is now written into CAM, which is used by all physical ports sharing the same policy.
Reset the Standby Unit in a Stack: The S-Series stacking feature set now supports the ability to reset the standby unit by running the reset command from the standby unit.
RIP: The FTOS RIPv1/v2 feature set is now available on the S-Series. Scalability and performance differences exist due to differences in the hardware architecture of each platform.
Save Task Exception Information: The FTOS serviceability feature set on the S-Series now saves exception information when there is an IPC communications failure on the master or standby unit. This enhancement will help to debug potential IPC problems faster and with less disruption to running systems. This feature is also available in FTOS 7.7.1.1.
Save to File Option for CLI Show Commands: The FTOS "show" commands are extended with a save option to save output to a file on flash for later use.
Secure DHCP — DHCP Relay Agent with Option 82: The DHCP relay agent with option 82 is a component of the FTOS secure DHCP suite of enterprise security features for establishing the legitimacy of DHCP servers and clients, and preventing DoS attacks and IP spoofing. RFC 3046 specifies option 82, which enables the DHCP relay agent (FTOS device) to include information about itself and the client when forwarding DHCP requests from a DHCP client to a DHCP server. The DHCP server uses the relay agent information to identify a client and assign an IP address based on the interface, rather than the client's MAC address.
Secure DHCP - DHCP Snooping: DHCP snooping is a component of the FTOS secure DHCP suite of enterprise security features for establishing the legitimacy of DHCP servers and clients, and preventing DoS attacks and IP spoofing. DHCP snooping builds and maintains a DHCP binding table and then validates all DHCP packets against this table.
Secure DHCP — IP Source Guard: IP source guard is a component of the FTOS secure DHCP suite of enterprise security features for establishing the legitimacy of DHCP servers and clients, and preventing DoS attacks and IP spoofing. IP source guard prevents IP spoofing by snooping DHCP traffic and then only permitting the IP addresses that were allocated with DHCP on the port to access the network.

Table 2: New Software Features for the S-Series (continued)

sFlow SNMP Set Configuration: The FTOS implementation of the sFlow MIB is enhanced to support sFlow configuration via SNMP sets.
Show Boot Code Version on Stack Units: The boot code version of a stack unit is now displayed in the **show system stack-unit** command for easier system software and inventory management.
Show LLDP System Name in CLI Commands: FTOS will now show system names in LLDP CLI show commands. Previous versions of FTOS displayed the chassis ID (for example, 00:01:e8:0d:b6:d6) in place of the system name. This feature was also introduced in FTOS 7.7.1.1.
Show Software Trace Files on Stack Members: The FTOS serviceability feature set on the S-Series is extended with the **show trace stack-unit** command, which shows software trace logs on stack units. Software traces are used to debug potential software problems without disrupting a running system. This feature is also available in FTOS 7.7.1.1.
SNMP Set Configuration Copy of Startup to Running: The enterprise-specific FORCE10-COPY-CONFIG-MIB supports SNMP set requests. FTOS 7.8.1.0 extends this MIB with support for copying the startup-config file to the running-config.
Stack Link Integrity Monitoring: S-Series units in a stacked configuration now monitor the integrity of stack ports, and disable any stack port that flaps five times within 10 seconds. Log messages appear on the console of the units that detect the flapping port. This feature was also introduced in FTOS 7.7.1.1.
Test CAM Capacity: The **test cam-usage** command is now available on the S-Series. Running this command before applying a QoS policy will show if there is enough room in CAM to accommodate the policy.
User-configurable Buffer Profile Templates: Buffer configuration commands are used to change the way a switch/router allocates packet buffers from its available memory, which helps to prevent packet drops during a temporary burst of traffic. The buffer configuration feature is enhanced with several profile templates that make changing the buffer allocation simpler.
User-configurable Buffer Settings for Control Queues: Buffer tuning commands are used to change the default way a switch/router allocates packet buffers from its available memory, which help to prevent packet drops during a temporary burst of traffic. This feature is enhanced to support configuring custom buffering for control plane queues. This feature was also introduced in FTOS 7.7.1.1.
Visual Indication of Master and Standby Status: The stacking LED display on each member of a stack will now indicate if the unit is the master or standby next to the stack unit number, so that these units can be identified visually. This feature is also available in FTOS 7.7.1.1.
VU#472363/CVE-2008-2476 IPv6 Neighbor Discovery Corruption of Routing Table: The FTOS IPv6 implementation is modified to drop invalid ND packets, which prevents forwarding table corruption as described in this vulnerability report. This change was also introduced in FTOS 7.7.1.1.
VU#800113/CVE-2008-1447 Multiple DNS Implementations Vulnerable to Cache Poisoning: The DNS client functionality in FTOS is enhanced so that DNS lookups now use random source UDP ports and random transaction IDs, to prevent spoofed DNS responses from being accepted. The DNS client is only enabled if the ip domain-lookup command is present in the configuration. This change was also introduced in FTOS 7.7.1.1.
Watchdog Timer: A hardware watchdog mechanism is introduced to automatically reboot an S-Series system that is unresponsive. This is a last resort mechanism intended to prevent a manual power cycle, and can be enabled on a standalone or stack of units. This feature is also available in FTOS 7.7.1.1.

S-Series Software Upgrade Procedures

S-Series systems are shipped with an FTOS image already loaded. However, you may want to upgrade your current FTOS image to a more recent FTOS image. This section contains three upgrade procedures:

- Upgrading from FTOS 7.6.1.0 to FTOS 7.7.1.1 on page 8
- Upgrading from FTOS 7.7.1.0 to FTOS 7.7.1.1 on page 11
- Upgrading to FTOS 7.8.1.0 on page 14
- Upgrading the S-Series Boot Code on page 16

Converting between SFTOS and FTOS

Converting between SFTOS and FTOS is separate from the following FTOS only upgrade procedure. The SFTOS to FTOS conversion process is documented in *Migrating and Understanding the Differences between the SFTOS and FTOS Operating Systems for the S-Series*, which is included in the software installation package, and is available on the Force10 website.

Upgrading from FTOS 7.6.1.0 to FTOS 7.7.1.1

Caution: Force10 recommends that you have at least 16 MB of memory when running FTOS version 7.6.1.0 or 22 MB when running version 7.7.1.1 before upgrading the system image on a ***stand-alone*** unit. Display the available memory on a unit using the **show processes memory stack-unit 0** command. If you have less than the recommended available memory, reduce the size of your configuration to free memory before upgrading.

Caution: Force10 recommends that you have at least 34 MB of memory when running version 7.7.1.1 before upgrading the system image on ***stacked units***. Display the available memory on a unit using the command **show processes memory stack-unit 0**. If you have less than the recommended available memory, reduce the size of your configuration to free memory before upgrading.

To upgrade the S-Series from FTOS 7.6.1.0 to 7.7.1.1:

Step	Task	Command	Mode
	Force10 recommends that you back up your startup configuration and any important files or directories to an external media prior to upgrading the system.		
1.	Verify that you have access to the FTP server containing the intermediate image file *FTOS-SB-7.6.1.0-INT.bin*, the boot code file *u-boot.2.8.1.0.bin*, and the FTOS image to which you are upgrading, *FTOS-SB-7.7.1.1.bin*.		
2.	Upgrade the boot flash image, as shown in Figure 2.	**upgrade boot ftp:**//*userid*:*password*@*hostip*/ *filepath*	EXEC Privilege

Figure 2 Upgrading the Boot Flash Image via FTP

```
Force10#upgrade boot ftp://myname@10.11.1.1//home/myname/u-boot.2.8.1.0.bin

!!!!!!!
Erasing SSeries BootImageUpgrade Table of Contents, please wait
.!.......................................................................!
1048576 bytes successfully copied
```

Step	Task	Command	Mode
3.	Upgrade to the intermediate system image, as shown in Figure 3.	**upgrade system ftp://***userid*:*password*@*hostip*/*filepath*	EXEC Privilege

Figure 3 Upgrading to the Intermediate System Image via FTP

```
Force10#upgrade system ftp://myname@10.11.1.1//home/myname/FTOS-SB-7.6.1.0-INT.bin

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Erasing Sseries ImageUpgrade Table of Contents, please wait
.!........................................................................................
..........................................................................................
..........................................................................................
..........................................................................................
..........................................................................................
..........................................................................................
..........................................................................................
..........................................................................................
!
```

Step	Task	Command	Mode
4.	Upon a successful completion of the copy process, reload the unit, as shown in Figure 4.	**reload**	EXEC Privilege

Figure 4 Reloading the S-Series

```
Force10#reload
Proceed with reload [confirm yes/no]: yes
.00:09:11: %STKUNIT0-M:CP %CHMGR-5-RELOAD: User request to reload the chassis
```

Step	Task	Command	Mode
5.	Verify that the unit is running *FTOS-SB-7.6.1.0-INT.bin*.	**show version**	EXEC Privilege
6.	Upgrade to FTOS version 7.7.1.1, as shown in Figure 5.	**upgrade system ftp://***userid*:*password*@*hostip*/*filepath*	EXEC Privilege

Figure 5 Upgrading the FTOS Image via FTP

```
Force10#upgrade system ftp://myname@10.11.1.1//home/myname/FTOS-SB-7.7.1.1.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Erasing Sseries ImageUpgrade Table of Contents, please wait
!.............................................................................
.!........................................................................................
..........................................................................................
.........................................................................................
..........................................................................................
..........................................................................................
..........................................................................................
!

14275705 bytes successfully copied
Force10#
```

Step	Task	Command	Mode
7.	Upon a successful completion of the copy process, reload the unit, as shown in Figure 4.	**reload**	EXEC Privilege

Step	Task	Command	Mode
8.	Verify that the unit is running FTOS version 7.7.1.1.	**show version**	EXEC Privilege
9.	Clear file system sectors (recommended)	**format flash:** You must include the colon (:) when entering this command.	EXEC Privilege
	Caution: The **format flash:** command deletes all files, including Configuration files.		
10.	Write the running configuration to the memory, and create the startup-config file.	**write mem**	Exec Privilege

After reloading the unit, FTOS displays the "InValid Magic" and "System ready" messages shown in Message 1 to indicate that the NVRAM is erased, as expected.

Message 1 InValid Magic and System Ready

```
Software Image[3] Hdr Checksum  : 0xb9c13975
Software Image[3] Data Checksum : 0x8164655b
Starting Force10 application

S_SERIES: SSNvInit - InValid Magic, so reset the NV structure.
S_SERIES: SSNvInit - InValid Magic, so reset the NV structure.

00:00:16: %STKUNIT0-M:CP %CHMGR-5-SYSTEM_READY: System ready
```

Erasing the NVRAM affects the following configurations:

- chassisSerialNum—FTOS automatically reads the serial number from EEPROM and updates it in the NVRAM if there is a mismatch.
- Last reload reason—FTOS erases this value if the unit was last reloaded by the user.
- SSH—SSH host keys are stored in NVRAM. FTOS regenerates then when FTOS applies the startup-config and the ip ssh server enable configuration. However, if the SSH client has "Strict Host Key" checking enabled, the SSH client denies access to the FTOS SSH server. To resolve this issue, you must modify the SSH client settings so that it uses the new key.

Upgrading from FTOS 7.7.1.0 to FTOS 7.7.1.1

Caution: Force10 recommends that you have at least 22 MB when running version 7.7.1.0 before upgrading the system image on a ***stand-alone*** unit. Display the available memory on a unit using the command **show processes memory stack-unit 0**. If you have less than the recommended available memory, reduce the size of your configuration to free memory before upgrading.

Caution: Force10 recommends that you have at least 34 MB of memory when running version 7.7.1.0 before upgrading the system image on ***stacked units***. Display the available memory on a unit using the command **show processes memory stack-unit 0**. If you have less than the recommended available memory, reduce the size of your configuration to free memory before upgrading.

Step	Task	Command	Mode
	Force10 recommends that you back up your startup configuration and any important files or directories to an external media prior to upgrading the system.		
1.	Upgrade to FTOS version 7.7.1.1, as shown in Figure 6.	**upgrade system ftp://** *userid*:*password*@*hostip*/*filepath*	EXEC Privilege

Figure 6 Upgrading the FTOS Image via FTP - Standalone unit

```
Force10#upgrade system ftp:
Address or name of remote host []: 10.10.10.10
Source file name []: E7.7.1/E7.7.1.1/FTOS-SB-7.7.1.1.bin
User name to login remote host: ftp
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing Sseries ImageUpgrade Table of Contents, please wait
!..........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...!
14563252 bytes successfully copied
Force10#
```

2.	For stacking, propagate the upgrade to all stacked units.	**upgrade system stack-unit all**	EXEC Privilege

Figure 7 Upgrading the FTOS Image via FTP - Stacked units

```
Force10#upgrade system ftp:
Address or name of remote host []: 10.10.10.10
Source file name []: E7.7.1/E7.7.1.1/FTOS-SB-7.7.1.1.bin
User name to login remote host: ftp
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing Sseries ImageUpgrade Table of Contents, please wait
!...........................................................................................
............................................................................................
............................................................................................
............................................................................................
!
14563252 bytes successfully copied
Force10#

Force10#upgrade system stack-unit all
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

3. Upon a successful completion of the copy process, reload the unit. **reload** EXEC Privilege

Figure 8 Reloading the S-Series

```
Force10#reload
Proceed with reload [confirm yes/no]: yes
.00:09:11: %STKUNIT0-M:CP %CHMGR-5-RELOAD: User request to reload the chassis
```

4. Verify that the unit is running FTOS version 7.7.1.1. **show version** EXEC privilege

Figure 9 Output example for **show version** command

```
Force10#show version
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: E7.7.1.1
Copyright (c) 1999-2008 by Force10 Networks, Inc.
Build Time: Fri Sep 12 10:58:00 PDT 2008
Build Path: /sites/sjc/work/sw/build/build4/Release/E7-7-1/SW/SRC
R6 uptime is 1 week(s), 2 day(s), 9 hour(s), 39 minute(s)

System Type: S50V
Control Processor: MPC8451E with 254361600 bytes of memory.

32M bytes of boot flash memory.

  1 48-port E/FE/GE with POE (SB)
 48 GigabitEthernet/IEEE 802.3 interface(s)
Force10#
```

5. Clear file system sectors (recommended) **format flash:** EXEC privilege

You must include the colon (:) when entering this command.

Caution: The **format flash:** command deletes all files, including Configuration files. Please implement the write mem command (step 5) to rebuild the startup-config.

6.	Write the running configuration to the memory, and create the startup-config file.	**write mem** If this command is not entered, configuration settings will be lost when the system is reloaded.	Exec privilege

After reloading the unit, FTOS displays the “InValid Magic” and “System ready” messages shown in Message 2 to indicate that the NVRAM is erased, as expected.

Message 2 InValid Magic and System Ready

```
Software Image[3] Hdr Checksum  : 0xb9c13975
Software Image[3] Data Checksum : 0x8164655b
Starting Force10 application

S_SERIES: SSNvInit - InValid Magic, so reset the NV structure.
S_SERIES: SSNvInit - InValid Magic, so reset the NV structure.

00:00:16: %STKUNIT0-M:CP %CHMGR-5-SYSTEM_READY: System ready
```

Erasing the NVRAM affects the following configurations:

- chassisSerialNum—FTOS automatically reads the serial number from EEPROM and updates it in the NVRAM if there is a mismatch.
- Last reload reason—FTOS erases this value if the unit was last reloaded by the user.

SSH—SSH host keys are stored in NVRAM. FTOS regenerates them when FTOS applies the startup-configuration and the **ip ssh server enable** configuration. However, if the SSH client has “Strict Host Key” checking enabled, the SSH client denies access to the FTOS SSH server. To resolve this issue, you must modify the SSH client settings so that it uses the new key.

Caution: FTOS 7.7.1.1 users upgrading from 7.7.1.0 a may lose stacking configuration information if the Master Priority and Unit Numbers are configured differently from the default assignments. Master, Standby and Member units will be reassigned to the default settings during the upgrade process, causing unpredicatable configuration issues.

Upgrading to FTOS 7.8.1.0

Caution: FTOS 7.8.1.0 is accompanied by a new boot code — **2.8.1.1**. FTOS 7.8.1.0 must be installed on the switch before installing the new boot code because older system images have a restriction on the size of the boot code that excludes boot code 2.8.1.1. Attempting to install the boot code first will result in messages similar to the following

```
% Error: Failed to save FTOS image release record to file.
% Error: Upgrade Boot image failed.
```

See Upgrading the S-Series Boot Code on page 16.

Caution: When your system is running version **7.7.1.0**, Force10 recommends that it have at least 22 MB free CPU memory before upgrading the system image on a ***stand-alone unit*** and at least 34 MB free CPU memory before upgrading the system image on ***stacked units***.

Caution: When your system is running version **7.7.1.1**, Force10 recommends that it have at least 22 MB free CPU memory before upgrading the system image on a ***stand-alone unit*** or on ***stacked units***.

Display the available memory on a unit using the command **show processes memory stack-unit 0**. If you have less than the recommended available memory, reduce the size of your configuration to free memory before upgrading.

Caution: Force10 recommends that your system have at least 22 MB free CPU memory when running version 7.8.1.0 before upgrading the system image on a ***stand-alone unit*** or on ***stacked units***.

Step	Task	Command	Mode
	Force10 recommends that you back up your startup configuration and any important files or directories to an external media prior to upgrading the system.		
1.	Upgrade to FTOS version 7.8.1.0, as shown in Figure 6.	**upgrade system ftp://** *userid:password@hostip/filepath*	EXEC privilege

Figure 10 Upgrading the FTOS Image via FTP - Standalone unit

```
Force10#upgrade system ftp:
Address or name of remote host []: 10.10.10.10
Source file name []: E7.8.1/E7.8.1.0/FTOS-SB-7.8.1.0.bin
User name to login remote host: ftp
Password to login remote host:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing Sseries ImageUpgrade Table of Contents, please wait
!..........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...........................................................................................
...!
14563252 bytes successfully copied
Force10#
```

Step	Task	Command	Mode
2.	For stacked units, propagate the upgrade to other units.	**upgrade system stack-unit** {**all** | **0-7**}	EXEC privilege

Figure 11 Upgrading the FTOS Image via FTP - Stacked Units

```
Force10#upgrade system stack-unit all
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

3. Upon a successful completion of the copy process, reload the unit. **reload** EXEC privilege

Figure 12 Reloading the S-Series

```
Force10#reload
Proceed with reload [confirm yes/no]: yes
.00:09:11: %STKUNIT0-M:CP %CHMGR-5-RELOAD: User request to reload the chassis
```

4. Verify that the unit is running FTOS version 7.8.1.0. **show version** EXEC privilege

Figure 13 Output example for **show version** command

```
Force10#show version
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: E7.8.1.0
Copyright (c) 1999-2008 by Force10 Networks, Inc.
Build Time: Fri Sep 12 10:58:00 PDT 2008
Build Path: /sites/sjc/work/sw/build/build4/Release/E7-7-1/SW/SRC
R6 uptime is 1 week(s), 2 day(s), 9 hour(s), 39 minute(s)

System Type: S50V
Control Processor: MPC8451E with 254361600 bytes of memory.

32M bytes of boot flash memory.

  1 48-port E/FE/GE with POE (SB)
 48 GigabitEthernet/IEEE 802.3 interface(s)
Force10#
```

5. Clear file system sectors (recommended) **format flash:** EXEC privilege

You must include the colon (:) when entering this command.

Caution: The **format flash:** command deletes all files, including Configuration files. Please implement the **write mem** command (step 6) to rebuild the startup-config.

6. Write the running configuration to the memory, and create the startup-config file. **write mem** EXEC privilege

If this command is not entered, configuration settings will be lost when the system is reloaded.

SSH — SSH host keys are stored in NVRAM. FTOS regenerates then when FTOS applies the startup-config and the ip ssh server enable configuration. However, if the SSH client has “Strict Host Key” checking enabled, the SSH client denies access to the FTOS SSH server. To resolve this issue, you must modify the SSH client settings so that it uses the new key.

Caution: FTOS 7.8.1.0 users upgrading from 7.7.1.0a may lose stacking configuration information if the Master Priority and Unit Numbers are configured differently from the default assignments. Master, Standby and Member units will be reassigned to the default settings during the upgrade process, causing unpredicatable configuration issues.

Upgrading the S-Series Boot Code

FTOS 7.8.1.0 is accompanied by a new boot code — 2.8.1.1. Force10 recommends this upgrade, but it is not mandatory. The new boot code enables you to boot the system from an FTOS image residing on a network TFTP source. For details on using the Network Boot facility, see the “Recovering from a Failed Start” section of the Management chapter in the *FTOS Configuration Guide for the S-Series.*

Boot code 2.8.1.1 is backward-compatible with FTOS 7.7.1.1, but the Network Boot facility is only supported by booting from an FTOS 7.8.1.0 image.

Other features included with boot code 2.8.1.1 include:

- Hardware watchdog support in u-boot. If the u-boot mode is idle for 64 seconds, then the box resets itself.
- The OK status LED starts blinking as soon as the box is powered up.
- Password recovery commands are available in BOOT_USER mode (bli mode): **ignore enable password**, **ignore startup-config**
- **restore factory defaults** command available in bli mode.
- Other BOOT_USER commands are available. See the BOOT_USER Mode chapter in the *FTOS Command Reference for the S-Series.*

Caution: FTOS 7.8.1.0 must be installed on the switch before installing the new boot code because older system images have a restriction on the size of the boot code that excludes boot code 2.8.1.1. Attempting to install the boot code first will result in messages similar to the following

```
% Error: Failed to save FTOS image release record to file.
% Error: Upgrade Boot image failed.
```

See FTOS 7.8.1.0 Software Features on page 5.

Caution: The boot code upgrade for the non-management members of a stack cannot be accomplished using the **upgrade boot stack-unit all** command. Instead, you must separate the stack members and upgrade them as standalone units, and then rejoin them into a stack. This issue is tracked in PR 80924.

Step	Task	Command	Mode
1.	Upgrade the switch/stack to FTOS 7.8.1.0	**upgrade system** See Upgrading to FTOS 7.8.1.0 on page 14.	EXEC privilege
2.	Reboot the system so that it boots up using the FTOS 7.8.1.0 image.	**reload**	EXEC privilege
3.	Separate stack members and upgrade each switch separately to boot code 2.8.1.1.	**upgrade boot** {**ftp** | **scp** | **tftp**} *url* After entering the source keyword, you can either follow it with the full *url* location of the source file in this form: //userid:password@hostip/filepath or Press **Enter** to launch a prompt sequence.	EXEC privilege
4.	Reboot the system.	**reload**	EXEC privilege

Step	Task	Command	Mode
5.	Verify that the new boot code is installed. The Boot Flash field displays the version as 2.8.1.1. **Note**: A boot code image earlier than 2.8.1.1 displays "Present" in the Boot Flash field, even if FTOS 7.8.1.0 is installed.	**show system stack-unit**	EXEC privilege
6.	Rejoin stack members.		

Using the **upgrade boot** command is shown in Figure 14:

Figure 14 Upgrading the Boot Code on S-Series

```
Force10#upgrade boot ?
ftp:                    Copy from remote file system (ftp://userid:password@hostip/filepath)
scp:                    Copy from remote file system (scp://userid:password@hostip/filepath)
tftp:                   Copy from remote file system (tftp://hostip/filepath)
Force10#$upgrade boot ftp://username:password@10.11.1.1/u-boot.2.8.1.1.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Erasing Sseries ImageUpgrade Table of Contents, please wait
.!..........................................................................................
............................................................................................
............................................................................................
............................................................................................
............................................................................................
............................................................................................
............................................................................................
............................................................................................
............................................................................................
............................................................................................
................!
12946259 bytes successfully copied
Force10#reload
```

Documentation Errata

The following updates are corrections or additions to the documentation:

- **Jumbo Frames**: S-Series are, by default, capable of handling jumbo frames, so references in Force10 user documentation to a non-jumbo mode do not pertain to S-Series (only to E-Series).
- **AAA Authentication Timeouts** — There are two timeouts, one between attempts to reach a sequence of TACACS or RADIUS servers, and the second between methods. The user guides only mention the configurable timeout between servers. In FTOS 7.8.1.0, there is a set 40-second timeout between methods.

  A method timeout is the time that FTOS will allow one authentication method to be unsuccessfully attempted before FTOS switches to the next method in the list.

  For example, if your authentication method list consists of three TACACS+ servers, followed by a RADIUS server, followed by local authentication, and you set the timeout between TACACS servers at 15 seconds, FTOS allows the first two TACACS+ server timeouts to complete, but will interrupt the third TACACS+ server connection attempt at 10 seconds (15+15+10= 40-second method timeout) to go to the RADIUS method. The attempt to reach the RADIUS server will time out at the limit you set with the **radius-server timeout** command, up to the 40-second method timeout.

Caveats

The following sections describe problem report (PR) types, and list open, closed, and rejected PRs:

- Caveat Definitions on page 18
- Resolved S-Series Hardware Caveats on page 19
- Open S-Series Hardware Caveats on page 19
- Rejected S-Series Software Caveats on page 19
- Resolved S-Series Software Caveats on page 19
- Open S- Series Software Caveats on page 30

➡ **Note:** Customers can subscribe to caveat update reports or use the BugTrack search tool to read current information about open and closed software caveats. To subscribe or use BugTrack, visit iSupport at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx. BugTrack currently tracks software caveats opened in FTOS version 6.2.1.1 and later.

All Release Notes are available on the Software Center tab of iSupport. The link to the relevant Release Notes for each software version is next to the link for that version:

https://www.force10networks.com/CSPortal20/Software/Downloads.aspx

Caveat Definitions

Category	Description
PR#	Problem Report number identifies the caveat.
Synopsis	Synopsis is the title or short description of the caveat.
Release Note	Release Notes contain more detailed information about the caveat.
Rejected	A section containing bugs published as open in previous Release Notes that have been subsequently found to be invalid, reproducible, or not otherwise scheduled for resolution.
Work Around	Work Around describes a mechanism for circumventing, avoiding, or recovering from the caveat. It might not be a permanent solution. Caveats listed in the “Closed Caveats” section should not be present, and the workaround is unnecessary, as the version of code for which this release note is documented has resolved the caveat.
Severity	**S1**—Crash: A software crash occurs in the kernel or a running process that requires a restart of the router or process. **S2**—Critical: A caveat that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no workaround acceptable to the customer. **S3**—Major: A caveat that effects the functionality of a major feature or negatively effects the network for which there exists a workaround that is acceptable to the customer. **S4**—Minor: A cosmetic caveat or a caveat in a minor feature with little or no network impact for which there might be a workaround.

Resolved S-Series Hardware Caveats

None

Open S-Series Hardware Caveats

None

Rejected S-Series Software Caveats

Caveats that appear in this section were reported in FTOS 7.7.1.0 as open, but have since been rejected. Rejected caveats are those that are found to be invalid, not reproducible, or not scheduled for resolution.

Resolved S-Series Software Caveats

Resolved caveats are those that have been listed in previous release notes and have been fixed in this FTOS version.

FIB (Resolved)

PR# 78268

Severity:	S2
Synopsis:	The "%FIB6-2-FIB6_HW_WRITE_ERROR: Failed to write entry into Host table" error message may be seen when traffic is being flooded during network loop.
Release Notes:	The "%FIB6-2-FIB6_HW_WRITE_ERROR: Failed to write entry into Host table" error message may be seen when traffic is being flooded through the unit in a network loop scenario.
Workaround:	None.

PR# 78282

Severity:	S3
Synopsis:	The CAM entries for a port-channel interface will be displayed incorrectly.
Release Notes:	The CAM entries for a port-channel interface will be displayed incorrectly if the interface includes member interfaces on unit 1 in a stack. This issue will not manifest if the member interfaces are on other units in a stack.
Workaround:	None. This issue is a display issue only. Traffic flow should remain unaffected.

PR# 78594

Severity:	S2
Synopsis:	Host moves to a new interface may lead to a mismatch between the FIB and CAM entries for those hosts.

Release Notes: Host moves to a new interface may lead to a mismatch between the FIB and CAM entries for those hosts.

Workaround: Execute the "clear arp-cache no-refresh" command.

Layer 3 ACL (Resolved)

PR# 79235

Severity: S2

Synopsis: If PVST in enabled on 10G interface, it may not forward traffic on S-Series switches.

Release Notes: If PVST in enabled on 10G interface, it may not forward traffic on S-Series switches.

Workaround: Use MSTP/RSTP instead. For adding tagged ports in this configuration,assign ip add, no shut vlan and then add tag ports.

MSTP (Resolved)

PR# 79572

Severity: S1

Synopsis: Spanning-tree state transition of blocking ports from an E-Series core to an S-Series distribution layer may result in a temporary loop.

Release Notes: Spanning-tree state transition of blocking ports from an E-Series core to an S-Series distribution layer may result in a temporary loop.

Workaround: Break the loop by shut/no-shutting the redundant Layer-2 path.

Multicast (Resolved)

PR# 77830

Severity: S2

Synopsis: IGMP snooping on stacked units is not supported.

Release Notes: IGMP snooping on stacked units is not supported.

Workaround: None. Note that IGMP snooping on non-stacked units is supported.

NTP (Resolved)

PR# 77132

Severity: S3

Synopsis: The system's calendar time will not be updated with UTC timezone for the time range 20:00 hrs - 23:00 hrs.

Release Notes: The system's calendar time will not be updated with UTC timezone for the time range 20:00 hrs - 23:00 hrs.

Workaround: Configure the timezone and then apply the calendar time.

OS / OS Infrastructure (Resolved)

PR# 73940

Severity: S2

Synopsis: Using the "speed 100" command on an S25P interface with multi-rate copper SFPs is not supported and will bring down the interface.

Release Notes: Using the "speed 100" command on an S25P interface with multi-rate copper SFPs is not supported and will bring down the interface.

Workaround: None. A speed of 100 Mbps is not supported in this release.

PR# 75611

Severity: S2

Synopsis: During system boot, the Status and Unit ID LEDs do not illuminate.

Release Notes: During system boot, the Status and Unit ID LEDs do not illuminate.

Workaround: None.

PR# 77825

Severity: S4

Synopsis: The status of "fan 5" for S25V and S25N will display as "down" in the output of the "show environment" command.

Release Notes: The status of "fan 5" for S25V and S25N will display as "down" in the output of the "show environment" command.

Workaround: None. This output can be ignored as these models do not support a 5th fan.

PR# 77892

Severity: S3

Synopsis: Intermittently, the system may report "fan(s) failed" alarm messages in the "show alarms" command and syslog messages for non-existant fan trays.

Release Notes: Intermittently, the system may report "fan(s) failed" alarm messages in the "show alarms" command along with generation of corresponding syslogs for non-existent fan trays.

Workaround: None. Reloading the system should clear the false alarms.

PR# 77962

Severity: S2

Synopsis: Under rare circumstances, the system hostname changes to junk characters when SSH server is enabled.

Release Notes: Under rare circumstances, the system hostname changes to junk characters when SSH server is enabled.

Workaround: Reload the system without saving the configuration to prompt the system to rewrite the hostname configuration.

PR# 77998

Severity: S3

Synopsis: The "show interfaces linecard/stack-unit " command will not display information for all interfaces in the slot

Release Notes: The "show interfaces linecard/stack-unit " command will not display information for all interfaces in the slot

Workaround: Use the "show interface tengigabitethernet {slot#/port#}" command.

PR# 78178

Severity: S3

Synopsis: The "show alarm thresholds" command does not display values applicable to S-Series.

Release Notes: The "show alarm thresholds" command does not display values applicable to S-Series.

Workaround: See the hardware guide for the correct values.

PR# 78179

Severity: S3

Synopsis: The "show environment fan" command on the S-Series displays fan status as up or down; fan speed is not indicated.

Release Notes: The "show environment fan" command on the S-Series displays fan status as up or down; fan speed is not indicated.

Workaround: None.

PR# 78240

Severity: S3

Synopsis: The "show proc {mem | cpu} management-unit" commands will not return any output on a standalone unit if unit-number is not 0.

Release Notes: The "show proc {mem | cpu} management-unit" commands will not return any output on a standalone unit if unit-number is not 0.

Workaround: None.

PR# 78300

Severity: S1

Synopsis: Kernel crashes may result after upgrading an S-Series unit to FTOS version 7.7.1.0.

Release Notes: Some S-Series units undergo a kernel failure which drops them to a 'db' prompt. This condition may manifest upon upgrade, upon reboot, or during the normal course of operation for an S-Series unit which is running FTOS version 7.7.1.0.

Workaround: None. A reboot may recover the system.

PR# 78396

Severity: S3

Synopsis: Incorrect port numbers are displayed when a non-Force10 qualified XFPs are inserted or upon a reboot.

Release Notes: When a non-Force10 qualified XFP is inserted, an informaitonal message similar to "%S50N:0 %IFAGT-5-UNSUP_OPTICS: Non-qualified optics in slot 0 port 51" is printed. The displayed port numbers in this message do not map to the logical interface ID. For port number 0/49, the port number displayed is 24. For port number 0/50, the port number displayed is 25. For port number 0/51, the port number displayed is 50. For port number 0/52, the port number displayed is 51. However, the ports can be accessed by their actual numbers; that is, port 49 can be brought up by issuing a no shut on port 49 and not 24.

Workaround: None.

PR# 78600

Severity: S3

Synopsis: Print statements pointing to an "SS I2C DRV ERR" error may be seen on the console.

Release Notes: Print statements pointing to an "SS I2C DRV ERR" error may be seen on the console.

Workaround: None. In FTOS releases with a resolution of this PR, the messages will be captured in the output of "show logging driverlog".

PR# 78979

Severity: S3

Synopsis: The show interface transceiver command displays incorrect number for the interface in which the optics is used.

Release Notes: The SFP number displayed in the "show interface gigabitethernet {slot#/port#} transceiver" command output does not match to the actual port number. For example, for physical port 0/2, the output of this command will indicate "SFP 1".

Workaround: None. This issue does not exist on the E-Series or C-Series.

PR# 79034

Severity: S3

Synopsis: Spurious signals received on the console may lead to S-Series units dropping down into kernel(db>) mode.

Release Notes: Spurious signals received on the console may lead to S-Series units dropping down into kernel(db>) mode.

Workaround: Execute a manual reboot of the unit.

PR# 79119

Severity: S2

Synopsis: Default flow control settings should not be displayed in the output of the "show config" command.

Release Notes: Default flow control settings ("flowcontrol rx off tx off") should not be displayed in the output of the "show config" command since this command should not display any defaults.

Workaround: None. This is a cosmetic only issue.

PR# 79919

Severity: S2

Synopsis: RPM failover can result in ARP not being resolved for the VLAN which has a static LAG

Release Notes: RPM failover can result in ARP not being resolved for the VLAN which has a static LAG.

Workaround: Unconfigure and reconfigure the LAG from the VLAN.

QoS (Resolved)

PR# 79018

Severity: S2

Synopsis: When buffer profile is applied to all interfaces using range command, hardware registers are not correctly set for some interfaces

Release Notes: When a buffer profile is applied to all interfaces using the "interface range" command, the underlying hardware registers are not set correctly for some interfaces. Up to 4 minutes may be required to update the underlying hardware registers across all ports on all port pipes.

Workaround: Wait for 3 to 4 minutes for the registers to be updated.

PR# 79176

Severity: S2

Synopsis: Adding or removing a buffer-policy using the "interface range" command may cause traffic to slow down or stop if the flow-control is also configured

Release Notes: Adding or removing a buffer-policy using the "interface range" range command may cause traffic to slow down or stop if the "flow-control" command also is enabled.

Workaround: Force10 does not recommend applying or/and removing buffer-profile in real time scenarios.

sFlow (Resolved)

PR# 79107

Severity: S1

Synopsis: If an sFlow collector is reached through a default route, an S-Series unit will eventually reset.

Release Notes: If sFlow is enabled, and the collector is reached through default route, then the FIB task consumes memory, eventually resetting the unit.

Workaround: Add a static route to reach sFlow collector.

SNMP (Resolved)

PR# 78498

Severity: S2

Synopsis: Port number reported in SNMP query for MAC address table is two more than the actual port number in port-pipe 1.

Release Notes: If an SNMP query is done with OID 1.3.6.1.2.1.17.7.1.2.2.1.2, the port number reported in the result is two more than the actual port number in MAC address table. The incorrect port number is reported for port-pipe 1; it is correct for port pipe 0.

Workaround: None.

Spanning Tree (Resolved)

PR# 79345

Severity:	S1
Synopsis:	After enabling spanning-tree 0 in a particular sequence, issuing the 'show spanning-tree 0' command can lead to a system reset.
Release Notes:	When you enable spanning tree instance 0 in a particular sequence on 15 or more interfaces and then issue the "show spanning-tree 0" command, the system may reset.
Workaround:	None.

Stacking (Resolved)

PR# 77327

Severity:	S2
Synopsis:	Intermittently, a non-existent stack-unit may not able to be removed if a stack split occurs after a failover.
Release Notes:	Intermittently, a non-existent stack-unit may not able to be removed if a stack split occurs after a failover.
Workaround:	None.

PR# 77348

Severity:	S2
Synopsis:	After a stack split (stacking cable is removed), the port status on S25P switches may not be shown correctly.
Release Notes:	After a stack split (stacking cable is removed), the port status on S25P switches may not be shown correctly.
Workaround:	None.

PR# 77572

Severity:	S4
Synopsis:	A tree topology with stack units is not supported.
Release Notes:	A tree topology with stack units is not supported.
Workaround:	Use a ring or daisy-chain topology.

PR# 78003

Severity: S2

Synopsis: In a ring topology, if an intermediate stack-unit crashes while booting, traffic flow through that unit is not diverted to alternate path.

Release Notes: In a ring topology, if an intermediate stack-unit crashes while booting, traffic flow through that unit is not diverted to alternate path.

Workaround: Reset the unit.

PR# 78125

Severity: S2

Synopsis: In a stack of 6 to 8 units, the stack-unit with the highest MAC address or highest priority may not come up as master.

Release Notes: In a stack of 6 to 8 units, the stack-unit with the highest MAC address or highest priority may not come up as master. This condition is more likely to occur when S25Ps are used in the stack.

Workaround: Avoid placing S25Ps as the first unit in the stack.

PR# 78126

Severity: S3

Synopsis: Changing the clock or calendar using the "clock set" or "calendar set" commands applies the changes to only the master and standby stack-units.

Release Notes: Changing the clock or calendar using the "clock set" or "calendar set" commands applies the changes to only the master and standby stack-units and not to the other members. Consequently, if a stack member other than the standby is now made master, the configured clock/calendar vales are lost.

Workaround: Re-configure the clock settings on the new master.

PR# 78142

Severity: S3

Synopsis: Under very rare circumstances (generally only after failover), a "%SWP-2-NO MORE TIMEOUT" may be reported between the FTOS IFM and IFA tasks.

Release Notes: Under very rare circumstances (generally only after failover), a "%SWP-2-NO MORE TIMEOUT" may be reported between the FTOS IFM and IFA tasks. When this condition manifests, the interface will continue to forward traffic, but interface-related operations, such as shutting or no-shutting a port, will not take effect.

Workaround: Reload the system to recover ability to change interface-related settings.

PR# 78148

Severity: S2

Synopsis: Enabling the SSH server on the S-Series may fail.

Release Notes: Enabling the SSH server on the S-Series may fail. When this error occurs, syslog messages such as "%SSH-6-CONNECTION: Connection refused by server. No new session" may be reported.

Workaround: Try enabling it again.

PR# 78150

Severity: S2

Synopsis: S-Series EEPROM contents may get erased under very rare circumstances.

Release Notes: Under very rare circumstances, the S-Series EEPROM contents may be erased completely. Messages similar to the following may appear: "Erasing Sseries Eeprom Primary Table of Contents, please wait..."

Workaround: Reprogram the eeprom contents, including the chassis MAC address and other manufacturing information. Please contact your Force10 Networks technical support representative for assistance.

PR# 78153

Severity: S2

Synopsis: Re-numbering the stack-unit ID to the number of a unit which is booting may hang the stack.

Release Notes: Re-numbering the stack-unit ID to the number of a unit which is booting may hang the stack.

Workaround: Avoid changing stack-unit IDs when any units are booting.

PR# 78194

Severity: S3

Synopsis: Auto reboot commands will not be synced to the standby unit in a stack after a save and reload with auto reboot disabled.

Release Notes: Auto reboot commands will not be synced to the standby unit in a stack after a save and reload with auto reboot disabled.

Workaround: Re-enable auto-reboot with the "auto-reboot disable" command after reload to place the command in the standby unit's configuration.

PR# 78208

Severity: S3

Synopsis: Intermittently, SNMP queries for the chSysStackPortTable of the f10-ss-chassis.mib on S-Series may time out.

Release Notes: Intermittently, SNMP queries for the chSysStackPortTable of the f10-ss-chassis.mib on S-Series may time out.

Workaround: Increase the SNMP timeout value to 3 or 4 seconds and the SNMP retries value to 5.

PR# 78218

Severity: S2

Synopsis: A back-to-back split and merge of a stack is not recommended without assigning priority to all member units.

Release Notes: A back-to-back split and merge of a stack is not recommended without assigning priority to all member units. Not doing so may lead to unexpected behavior in the merged stack.

Workaround: Assign a priority before doing a back-to-back split and merge.

PR# 78237

Severity: S2

Synopsis: Under very rare circumstances NVRAM error/DATASYNC_FAIL Messages could be seen when the running config is being saved.

Release Notes: Under very rare circumstances NVRAM error/DATASYNC_FAIL Messages could be seen when the running config is being saved.(write memory/copy run start/saving the config during reload).

Workaround: --None ---

PR# 78259

Severity: S2

Synopsis: Under very rare circumstances, stack members may become stuck during boot or failover.

Release Notes: Under very rare circumstances, stack members may become stuck during boot or failover. When this condition manifests, the boot-up sequence messages suddenly stop appearing.

Workaround: Reload the system again to recover.

PR# 78273

Severity: S2

Synopsis: 4 Meter stacking cable for both 12g and 24g may cause packet drops with random data patterns

Release Notes: 4 Meter stacking cable for both 12g and 24g may cause packet drops with random data patterns

Workaround: None

PR# 79259

Severity: S2

Synopsis: 10GE ports of the XFP module may no longer appear in the "show run" output on the standby switch after consecutive stack resets.

Release Notes: 10GE ports of the XFP module may no longer appear in the "show run" output on the standby switch after consecutive stack resets. When this condition occurs, the module still should be recognized by the system.

Workaround: Reset the stack.

Open S- Series Software Caveats

CLI (Open)

PR# 77193

Severity: S2

Synopsis: A privilege level cannot be set for some interface-level commands.

Release Notes: A privilege level cannot be set for some interface-level commands. For example, assign a privilege level of two to the "flowcontrol" and "ip access-group" commands and then, once logged in with the appropriate privileges, attempt to configure either of these commands. A message of "% Error: Invalid input at "^" marker." will be returned.

Workaround: Use TACACS for command authorization.

PR# 77764

Severity: S4

Synopsis: The "copy running-config startup-config duplicate" command is not supported on the S-Series.

Release Notes: The "copy running-config startup-config duplicate" command is not supported on the S-Series. This command applies only to systems which have external flash.

Workaround: Avoid executing this command on the S-Series. Instead, on the S-Series, please perform a file copy operation via FTP/TFTP to extract the file.

PR# 78174

Severity: S2

Synopsis: Executing the same show | grep command simultaneously from two sessions may lead to a switch hung state.

Release Notes: Executing the same show | grep command simultaneously from two sessions may lead to a system hang state.

Workaround: Do not execute this command sequence from two sessions. If a system reaches the hung state, a reboot is required to recover.

Control Plane (Open)

PR# 80929

Severity: S2

Synopsis: L2 protocol packets may also be shown as "'Dropped by FP" in "show hardware" outputs.

Release Notes: Protocol packets for STP/LLDP/LACP/GVRP/ARP Reply/Dot1x/VRRP/GRAT ARP may be shown as "'Dropped by FP" in "show hardware" outputs.

Workaround: These drops can be ignored since actual protocol packets are being delivered to the right CPU in the system.

DHCP (Open)

PR# 79959

Severity: S2

Synopsis: Static entries may be removed from the snooping table on receiving a DHCPRELEASE within a snooped VLAN.

Release Notes: Static entries may be removed from the snooping table on receiving a DHCPRELEASE within a snooped VLAN. This issue can manifest only when the DHCPRELEASE matches to any IP or MAC in the snooping table.

Workaround: Re-enter the static entries.

PR# 81080

Severity: S1

Synopsis: A software exception may happen when enabling source-address-validation when the DHCP snooping binding table contains 1500 or more entries.

Release Notes: A software exception may happen when enabling source-address-validation when the DHCP snooping binding table contains 1500 or more entries

Workaround: Enable source address validation with the "ip dhcp source-address-validation" command when the snooping table entries are less than 1200 on a single interface.

PR# 81128

Severity: S2

Synopsis: The DHCP snooping table may not be populated when server-connected port-channel interface and the DHCP clients are in the same VLAN.

Release Notes: The DHCP snooping table may not be populated when server-connected port-channel interface and the DHCP clients are in the same VLAN.

Workaround: Use separate VLAN for the trust port if the server is connected via a port-channel interface.

FIB (Open)

PR# 73319

Severity: S2

Synopsis: The "show ip flow" and "show ip route" commands may display an invalid value in the "Egress Interface" field.

Release Notes: The "show ip flow" and "show ip route" commands may display an invalid value in the "Egress Interface" field. This primarily impacts the S-Series.

Workaround: None. This issue is a display issue only.

PR# 74341

Severity: S3

Synopsis: When the "load-balance" command is configured, the "show ip flow" command may display an incorrect egress port for some flows.

Release Notes: When the "load-balance" command is configured, the "show ip flow" command may display an incorrect egress port for some flows.

Workaround: None. This is a display issue only.

PR# 75028

Severity: S2

Synopsis: Executing the "clear ip fib" command with a large number of routes or "show ip ospf" may lead to a "%FIB6-2-FIB6_HW_WRITE_ERROR" condition.

Release Notes: On a system with a large number of ARPs routes (greater than 1k), executing the "clear ip fib' command may lead to an error message similar to "%STKUNIT0-M:CP %FIB6-2-FIB6_HW_WRITE_ERROR: Failed to write entry into Host table".

Workaround: None.

PR# 77250

Severity: S3

Synopsis: In an ECMP scenario, disabling one of the interfaces causes traffic loss on the remaining interfaces.

Release Notes: In an ECMP scenario, disabling one of the interfaces causes traffic loss on the remaining interfaces.

Workaround: Do not disable an interface when traffic loss cannot be tolerated.

PR# 79851

Severity: S3

Synopsis: Under rare circumstances, the egress port of static ARP entries will be inconsistent between the FIB and CAM of a linecard after a failover.

Release Notes: After an RPM or stack failover, the ARP manager process in FTOS may not contain all configured static ARP entries. The line card FIB may point to CP, instead of the correct egress interface.

Workaround: Reconfigure the static ARP entry after failover.

PR# 81056

Severity: S2

Synopsis: The "show ip fib" command will not display the VLAN ID for routes learned on a VLAN via BGP.

Release Notes: The "show ip fib" command will not display the VLAN ID for routes learned on a VLAN via BGP. It will show the correct egress port. This issue does not impact routes learned via routing protocols.

Workaround: Use the "show ip cam" command.

GVRP (Open)

PR# 74144

Severity: S2

Synopsis: Dynamic VLAN members assigned via GVRP are not removed when an interface is shut down.

Release Notes: Dynamic VLAN members assigned via GVRP are not removed when the vlan members are in shutdown state.

Workaround: Disable GVRP on the interface to clear the dynamic memberships.

IPv6 (Open)

PR# 80100

Severity:	S2
Synopsis:	The "show ipv6 cam" command will not display the VLAN ID for routes having next-hop as only VLAN egress interface.
Release Notes:	The "show ipv6 cam" command will not display the VLAN ID for routes having next-hop as only VLAN egress interface.
Workaround:	Use the "show ipv6 fib" command.

PR# 80872

Severity:	S2
Synopsis:	The "show ipv6 cam summary" displays total number of routing entries, rather than the number of entries actually installed in CAM.
Release Notes:	In a CAM full scenario during which IPv4 routes have filled the CAM and hence no IPv6 routes are actually installed, the "show ipv6 cam summary" command will display the number of prefixes equal to the number of routes in the routing table, rather than a count of routes actually installed in CAM.
Workaround:	None.

Layer 2 (Open)

PR# 72161

Severity:	S3
Synopsis:	The "1023-byte pkts" from the output of "show interface" may display higher than expected value.
Release Notes:	The "1023-byte pkts" output counter may display a higher than expected value as 64-byte packets are counted incorrectly as "1023-byte pkts".
Workaround:	None.

PR# 75539

Severity:	S3

Synopsis: The "show port-channel-flow" command may display the wrong interface when ingress and egress ports are in different port-pipe/line card.

Release Notes: The "show port-channel-flow" command may display the wrong interface when ingress and egress ports are in different port-pipe/line card.

Workaround: None.

PR# 75595

Severity: S3

Synopsis: The "show port-channel-flow" command may display wrong interface when ingress port is part of non-default VLAN.

Release Notes: The "show port-channel-flow" command may display wrong interface when ingress port is part of non-default VLAN.

Workaround: None.

Layer 3 ACL (Open)

PR# 75328

Severity: S2

Synopsis: ACL with the "count" option may display incorrect value when new rules are inserted in between while sending traffic.

Release Notes: If new rules are added in the middle of an existing ACL rule list while traffic is running and the ACL rules are configured with the "count" option, the ACL counters will display double the number of actual matching packets.

Workaround: None.

Logging (Open)

PR# 74777

Severity: S3

Synopsis: Booting messages are displayed in the "show logging" output

Release Notes: TSM log messages, such as "%TSM-6-PORT_CONFIG", which are suppressed during bootup will be written to the syslog file and be shown in the "show logging" command output after reload.

Workaround: Ignore these booting messages in "show log".

Multicast (Open)

PR# 79461

Severity:	S2
Synopsis:	Multicast replication may not work if a VLAN tagged interface is both ingress and egress port of a PIM (S,G) entry.
Release Notes:	When the incoming interface and outgoing interface of a PIM (S,G) entry are VLANs, and the same member port is tagged in both VLANs, replication of multicast packets on that port may not work.
Workaround:	None.

PR# 79474

Severity:	S2
Synopsis:	When Source and receivers are on the same VLAN, disabling IGMP snooping globally may show a traffic distruption to the hosts
Release Notes:	When Source and receivers are on the same VLAN, disabling IGMP snooping globally may show a traffic distruption to the hosts
Workaround:	No Workaround

PR# 79476

Severity:	S3
Synopsis:	PIM TIB maynot have the (S,G) entry for dynamic groups in IGMPv2-Compat mode and when changed to IGMPv2 mode from IGMPv2Compat mode
Release Notes:	PIM TIB maynot have the (S,G) entry for dynamic groups in IGMPv2-Compat mode and when changed to IGMPv2 mode from IGMPv2Compat mode
Workaround:	No Workaround

PR# 79677

Severity:	S2
Synopsis:	User-initiated shut/no shut on a port-channel may disrupt multicast traffic
Release Notes:	If multicast receivers are connected to a port-channel interface and a shut / no-shut operation is made on the interface, multicast traffic to the interface may be disturbed.
Workaround:	None.

PR# 80008

Severity:	S3
Synopsis:	IGMPv3 host that requests for blocking of a multicast group may receive traffic if IGMPv2 host joins the same group with SSM-MAP.
Release Notes:	IGMPv3 host that requests for blocking of a multicast group may receive traffic if IGMPv2 host joins the same group with SSM-MAP.

Workaround: None.

MSTP (Open)

PR# 77848

Severity: S2

Synopsis: Disabling MSTP on a system with a relatively large MSTP configuration may lead to LACP port-channel interface flapping.

Release Notes: Disabling MSTP on a system with a relatively large MSTP configuration may lead to LACP port-channel interface flapping, as reported via messages similar to "%LACP-5-PORT-UNGROUPED: PortChannel-001-Ungrouped".

Workaround: None.

OS / OS Infrastructure (Open)

PR# 69981

Severity: S3

Synopsis: Frames larger than 9216 bytes will not be counted in the "over 1023-byte pkts" counter in the output of the "show interfaces" command.

Release Notes: Frames larger than 9216 bytes will not be counted in the "over 1023-byte pkts" counter in the output of the "show interfaces" command.

Workaround: None. The counter will increment for frames less than or equal to 9216 bytes.

PR# 72160

Severity: S2

Synopsis: Rate info may be incorrect from output of "show interfaces".

Release Notes: The calculated "Rate info" display in the "show interfaces" output will be lower than the actual rate. This condition can manifest with both small and large packet sizes and with the default and 30-second rate intervals.

Workaround: None.

PR# 72673

Severity: S1

Synopsis: Upgrading a system image is recommended only with free memory of 16 MB or more in FTOS Release 7.6.1 and 21 MB or more in FTOS Release 7.7.1.

Release Notes: Upgrading a system image on a standalone unit is recommended only with free memory of 16 MB or more in FTOS Release 7.6.1 and 21 MB or more in FTOS Release 7.7.1.

Workaround: Display available memory via the "show process memory management-unit" command. If required, reduce the size of the configuration so that at least the required amount of memory is free before initiating the upgrade procedure.

PR# 72932

Severity: S2

Synopsis: "CP running low on memory" messages may be seen on console when upgrading an image with initial free memory between 15 - 25 MB

Release Notes: Messages similar to "/netbsd: CP running low on memory, available memory 1650688 bytes" may be seen when upgrading an image while free memory was between ~15M and ~25M.

Workaround: Please ignore these messages. They will stop once the upgrade is done.

PR# 73160

Severity: S3

Synopsis: The total, used and free values displayed in the "show memory" command output may differ from the values shown in "show proc mem."

Release Notes: The total, used and free values displayed in the "show memory" command output may differ from the values shown in "show proc mem." This condition results from how each command accounts for memory usage.

Workaround: None.

PR# 74541

Severity: S3

Synopsis: Number of ports shown for base unit includes 10-GE ports in show system and syslog, even if 10-GE ports are not present.

Release Notes: The number of ports shown for a base unit will include 10-GE ports in the "show system" output and syslog even if such ports are not present in the system. For S50V and S50N, it will show 52 ports, and for S25P it will show 28 ports.

Workaround: Check the "show system" command to see whether the 10-GE module is present.

PR# 74819

Severity: S3

Synopsis: Corresponding combo copper interface may go down when certain fiber SFPs are inserted on the fiber interface.

Release Notes: When a combo copper interface on an S50V or S25P is connected to a 10/100 switch, inserting a fiber SFP from a particular vendor(s) on the corresponding fiber interface may cause the copper link to go down. This condition results from an issue with auto-negotiation. It has been seen with Finisar SFPs, and may occur with other SFPs from other vendors.

Workaround: Do not insert a fiber SFP into the fiber port if the corresponding copper combo port is connected to a 10/100 switch and is being used.

PR# 75017

Severity: S3

Synopsis: The "show proc mem" command will show higher values for free memory by approx 2 MB on the S-Series.

Release Notes: The "show proc mem" command will show higher values for free memory by approximately 2 MB on the S-Series.

Workaround: None.

PR# 75021

Severity: S3

Synopsis: On the S Series, SSH will take a longer than expected time to be enabled.

Release Notes: On the S Series, SSH will take a longer than expected time to be enabled.

Workaround: None.

PR# 75096

Severity: S2

Synopsis: In rare, unreproducible conditions, a portion of the configuration may be lost while the config file is copied from flash to the startup-config.

Release Notes: In rare, unreproducible conditions, a portion of the configuration may be lost while the config file is copied from flash to the startup-config.

Workaround: None.

PR# 77547

Severity: S3

Synopsis: With "no auto-neg" and "speed" commands on combo port, the "show int ten {slot#/port#}" command may show an incorrect speed.

Release Notes: If auto-negotiation is disabled on a combo card interface via the "no auto-neg" command and a speed setting is configured, the "show int ten {slot#/port#}" command may show an incorrect speed.

Workaround: Use the "show config" command to confirm your setting.

PR# 77684

Severity:	S3
Synopsis:	Partial configuration is saved upon "write memory" if insufficient space exists in flash. No syslog message is reported for Telnet sessions.
Release Notes:	If multiple, separate large configuration files are saved in flash and a 'write mem' is issued such that the complete file cannot be saved, only a partial configuration is written in the order it appears in the 'show running-config' file. A message similar to "FILEMGR-5-USRFLASHFULL: Warning! User flash device flash: is currently 100% full" is not reported to the Telnet session.
Workaround:	If you are writing multiple large config files to flash, check available memory.

PR# 77968

Severity:	S3
Synopsis:	The copper interface will experience a link flap when a Finisar SFP is inserted into the corresponding fiber interface slot.
Release Notes:	The copper interface will experience a link flap when a Finisar SFP is inserted into the corresponding fiber interface slot.
Workaround:	Avoid inserting the fiber SFP when a link flap cannot be tolerated.

PR# 78049

Severity:	S2
Synopsis:	Converting from FTOS 7.7.1.1 directly to SFTOS is not supported.
Release Notes:	Converting from FTOS 7.7.1.1 directly to SFTOS is not supported.
Workaround:	Downgrade to 7.7.1.0 first and then use the "upgrade system ftp:" command to convert back to SFTOS using the SFTOS-out.img image.

PR# 79367

Severity:	S3
Synopsis:	Alarm LED of standby unit in S-Series stack does not glow for standby generated alarms.
Release Notes:	Alarm LED of standby unit in S-Series stack does not glow for standby generated alarms.
Workaround:	None.

PR# 79439

Severity:	S2
Synopsis:	LACP sessions may flap when executing a "write memory" or when a "copy run flash:/" operation is executed on an S-Series' stack.
Release Notes:	LACP sessions may flap when executing a "write memory" or when a "copy run flash:/" operation is executed on an S-Series' stack. These issues have not been seen on S-Series' standalone units.
Workaround:	None.

PR# 79626

Severity:	S3

Synopsis: Front panel LED for 10G CX4 modules of S-Series do not glow when the port is up.

Release Notes: Front panel LED for 10G CX4 modules of S-Series do not glow when the port is up.

Workaround: None.

PR# 79714

Severity: S3

Synopsis: Discard counter value is twice the actual discarded number when a received frame size is greater than the configured MTU size.

Release Notes: When the line speed is 1000Mb/s, received frames greater than the MTU will cause the interface's discard counter value to increment two times for each frame.

Workaround: None.

PR# 79716

Severity: S3

Synopsis: Duplex configurations will not take effect on the copper SFP interfaces with "speed 10" and "no negotiation auto".

Release Notes: Duplex configurations will not take effect on the copper SFP interfaces with "speed 10" and "no negotiation auto".

Workaround: None.

PR# 79720

Severity: S3

Synopsis: Pause frames are not supported on the copper SFP for the S-Series.

Release Notes: Pause frames are not supported on the copper SFP for the S-Series. Such frames are supported on other platforms as well as on other interface types for the S-Series.

Workaround: None.

PR# 79721

Severity: S3

Synopsis: The configurations made when copper SFP is present will not take effect on copper combo ports after copper SFP is removed

Release Notes: The configurations made when copper SFP is present will not take effect on copper combo ports after copper SFP is removed

Workaround: None.

PR# 80069

Severity: S2

Synopsis: Booting the unit only from default boot parameter via tftp might not work at times as few letters from tftp filename will go missing after reload.

Release Notes: Booting the unit only from default boot parameter via tftp might not work at times as few letters from tftp filename will go missing after reload.

Workaround: Boot the unit via tftp using primary or secondary boot parameters.

PR# 80296

Severity: S2

Synopsis: Very rarely the unit might stop at boot user mode every time we reload if unit is booted with pre 7.8.1 system image and 2.8.1.1 boot code.

Release Notes: Very rarely the unit might stop at boot user every time we reload if unit is booted with pre 7.8.1 system image and 2.8.1.1 boot code.

Workaround: Execute "restore factory-defaults" command in BLI. This will solve the problem but will erase nvram data (ssh config,stack unit priority)/file system data(startup-config,files present under flash)/boot configurations(current boot parameters) as well.

PR# 80446

Severity: S3

Synopsis: On the S-Series, the "show process cpu" command...

Release Notes: In S-series chassis, "show processes cpu" or "show processes cpu stack-unit " shows the cpu utilization by Agent tasks(tasks running in member units),for the last 1 and 5 minutes for that particular stack unit. In case of a standalone or a management-unit the 5secs value corresponds to the CPU utilization by all processes, both Agent and Manager tasks. The actual CPU utilization by the entire Chassis(Standalone or the entire Stack) is shown in "show processes cpu management-unit" output.

Workaround:

PR# 80507

Severity: S3

Synopsis: The "show processes cpu management-unit" will not display the number of highest-CPU-usage tasks specified with the "Number of tasks" option.

Release Notes: The "show processes cpu management-unit" will not display the number of highest-CPU-usage tasks specified with the "Number of tasks" option. Instead, it will display the top 2 processes using CPU cycles.

Workaround: Execute the command without the number of tasks option.

PR# 80924

Severity: S2

Synopsis: Upgrading the boot code for the non-management members from the management unit is not supported.

Release Notes: Upgrading the boot code for the non-management members from the management unit is not supported for this release.

Workaround: Upgrade the boot code for each of the units individually before adding it to stack. Executing the command "upgrade boot stack-unit all" might result in corrupting the boot code of the non-management units.

PR# 81013

Severity: S3

Synopsis: The "Boot Flash" field for non-management units will display the boot code version of the management unit.

Release Notes: The "Boot Flash" field for non-management units will display the boot code version of the management unit.

Workaround: No workaround. Upgrade all units to same boot code versions as the management unit to avoid confusion.

PR# 81045

Severity: S2

Synopsis: "f10StkATPResetReq: Requesting ATP reset from: 4 reason: 4 disableAutoReboot 0" may be seen when "redundancy force-failover" is executed.

Release Notes: Messages similar to "f10StkATPResetReq: Requesting ATP reset from: 4 reason: 4 disableAutoReboot 0" may be seen when "redundancy force-failover" is executed in a stack of S-Series.

Workaround: These messages can be safely ignored.

PR# 81087

Severity: S2

Synopsis: Intermittently, the TFTP server configured from boot user mode might not be reachable after reload.

Release Notes: Intermittently, the TFTP server configured from boot user mode might not be reachable after reload.

Workaround: When this issue manifests, the sever address will be configured as a "Management Interface". Deleting this IP from the ARP table will resolve the issue.

OSPF (Open)

PR# 73339

Severity: S2

Synopsis: OSPF might get struck in EXSTART/DROTHER state if interface flaps during OSPF adjacency formation.

Release Notes: OSPF might get struck in EXSTART/DROTHER state if interface flaps during OSPF adjacency formation.

Workaround: None.

Port Monitoring (Open)

PR# 77554

Severity: S2

Synopsis: For outbound monitoring sessions with SRC ports on the same port-pipe, broadcast and unknown traffic will be mirrored to last-configured DEST port.

Release Notes: When two or more monitoring sessions have source ports in the same port-pipe and the destination ports for those sessions are different, then any flooded or broadcast traffic (layer 2 or layer 3) going out of the source ports will be mirrored only to the destination port of the session that was configured last for the source port-pipes under consideration.

Workaround: None.

PR# 77712

Severity: S2

Synopsis: Outgoing traffic will continue to be mirrored after an MD port transitions from the forwarding to blocking state in STP.

Release Notes: Outgoing traffic will continue to be mirrored after an MD port transitions from the forwarding to blocking state in STP.

Workaround: None.

PR# 78147

Severity: S1

Synopsis: Executing the command "no stack-unit {unit#} provision" with port mirroring on the same unit # may lead to a system failover to a standby unit.

Release Notes: Executing the command "no stack-unit {unit#} provision" may lead to a system failover to standby. This happens when the pre-configured unit has configurations related to port mirroring.

Workaround: If possible, remove the port mirroring configuration when using this command.

Power Over Ethernet (PoE) (Open)

PR# 78912

Severity: S2

Synopsis: The "no power inline" command does not remove the "power inline priority" command

Release Notes: The "no power inline" command does not remove the "power inline priority" command from the running configuration. Executing a "show config" will display that the "power inline priority" command remains enabled.

Workaround: Use "no power inline priority" separately to remove the power priority configuration.

PVST (Open)

PR# 78146

Severity: S3

Synopsis: Re-activating a PVST enabled interface causes the port to transition through all the PVST states

Release Notes: With PVST, enabling and disabling an interface causes the interface to transition through all PVST states before becoming a root or non-root port.

Workaround: None.

QoS (Open)

PR# 70029

Severity: S2

Synopsis: At all packet sizes, a significantly higher packet rate may be received than the rate set in the "storm-control unknown-unicast" command.

Release Notes: At all packet sizes, a significantly higher packet rate may be received than the rate set in the "storm-control unknown-unicast" command.

Workaround: None.

Security (Open)

PR# 74924

Severity: S2

Synopsis: NAS port id interpretation for 802.1x may not be uniform for all the ports.

Release Notes: NAS port id interpretation for 802.1x may not be uniform for all the ports.

Workaround: The NAS port id for 802.1x needs to be interpreted in the following way For S50: ----------- For Nas Port Id = 0 - 23, User Port Id = 1 - 24 For Nas Port Id = 24, 25, User Port Id = 49, 50 For Nas Port Id = 26 - 49, User Port Id = 25 - 48 For Nas Port Id = 50, 51, User Port Id = 51, 52 For S25: ----------- For Nas Port Id = N the User Port Id = N + 1

sFlow (Open)

PR# 76865

Severity: S2

Synopsis: When dot1p priority is set on incoming interface, the sFlow extended-switch dot1p value for egress sampled traffic will not include configured value.

Release Notes: When dot1p priority is set on an incoming interface, the sFlow extended-switch dot1p information for egress sampled traffic will not include the configured dot1p values. Instead, the sampled datagram will have the original incoming traffic priority.

Workaround: None.

PR# 77199

Severity: S3

Synopsis: sFlow datagrams for a second collector are dropped after disable/enable with two collectors having the same IP address and a different UDP port number

Release Notes: sFlow datagrams for a second collector are dropped after disable/enable with two collectors having the same IP address and a different UDP port number.

Workaround: None.

PR# 77946

Severity: S2

Synopsis: sFlow is not supported on an S-Series stack.

Release Notes: sFlow is not supported on an S-Series stack. sFlow on standalone units and on a master unit in a stack works as expected.

Workaround: None.

SNMP (Open)

PR# 73611

Severity: S2

Synopsis: The agent address will be shown as 0.0.0.0 for v1 traps on S-Series platforms.

Release Notes: The agent address will be shown as 0.0.0.0 for v1 traps on S-Series platforms.

Workaround: None.

PR# 75125

Severity: S3

Synopsis: stackUnitMacAddress OID for the S-Series' CHASSIS MIB may not return a value.

Release Notes: An snmpwalk on the stackUnitMacAddress OID (.1.3.6.1.4.1.6027.3.10.1.2.2.1.19) for the S-Series' CHASSIS MIB may not return a value.

Workaround: None.

PR# 78770

Severity: S3

Synopsis: chStackUnitMgmtStatus in FORCE10-SS-CHASSIS-MIB cannot be used to identify the standby unit.

Release Notes: chStackUnitMgmtStatus in FORCE10-SS-CHASSIS-MIB cannot be used to identify the standby unit. The returned value will be "stackUnit(2)" for the standby as well.

Workaround: None.

PR# 79154

Severity: S3

Synopsis: f10-ss-chassis-mib -> chStackUnitIndexNext is not implemented and will always return 1.

Release Notes: f10-ss-chassis-mib -> chStackUnitIndexNext is not implemented and will always return 1.

Workaround: None.

PR# 79156

Severity: S2

Synopsis: FORCE10-SS-CHASSIS-MIB - chSysProcessorTable returns rows only for management unit and ignores the other units in stack.

Release Notes: FORCE10-SS-CHASSIS-MIB - chSysProcessorTable returns rows only for management unit and ignores the other units in stack.

Workaround: None.

PR# 80835

Severity: S4

Synopsis: SNMP trap for authentication is not generated.

Release Notes: An authentication trap is not generated even when enabled by the command 'snmp-server enable traps snmp authentication'.

Workaround: None.

Spanning Tree (Open)

PR# 81077

Severity: S2

Synopsis: A Spanning Tree topology change will not be reported via an SNMP trap when SNMP traps are also enabled along with xstp traps.

Release Notes: A Spanning Tree topology change will not be reported via an SNMP trap when SNMP traps are also enabled along with xstp traps:

```
snmp-server enable traps snmp authentication coldstart linkdown linkup
snmp-server enable traps stp
snmp-server enable traps xstp
```

Workaround: Monitor the system using the equivalent syslog messages such as: %RPM0-P:CP %SPANMGR-5-STP_NEW_ROOT: New Spanning Tree Root. My Bridge Id: 32768:0001.e82d.7c82 Old Root: 32768:0000.0000.0000 New Root: 32768:0001.e82d.7c82.
%RPM0-P:CP %SPANMGR-5-STP_ROOT_CHANGE: STP root changed.
My Bridge ID: 32768:0001.e82d.7c82 Old Root: 32768:0000.0000.0000 New Root: 32768:0001.e82d.7c82

or Disable SNMP traps to receive xstp traps

Stacking (Open)

PR# 76610

Severity: S3

Synopsis: Invalid calculated rates for percentage of line rate may be shown in "show hardware stack-unit # cpu data-plane statistics stack-port #" output.

Release Notes: Invalid calculated rates for percentage of line rate may be shown in "show hardware stack-unit # cpu data-plane statistics stack-port #" output.

Workaround: None.

PR# 77349

Severity: S3

Synopsis: The "stack-unit {unit#} priority {value}" command is not displayed in the running configuration.

Release Notes: The "stack-unit {unit#} priority {value}" command is not displayed in the running configuration.

Workaround: Check the configured priority value with the "show system stack-unit {unit#}" command.

PR# 77519

Severity: S3

Synopsis: The alarm LED will not be set for stack members when a minor or major alarm is active.

Release Notes: The alarm LED will not be set for stack members when a minor or major alarm is active. The LED will be set correctly on the master unit.

Workaround: None.

PR# 77726

Severity: S1

Synopsis: Hot swap of S-Series' stacking modules is not supported and may lead to a system reset.

Release Notes: Hot swap of S-Series' stacking modules is not supported and may lead to a system reset.

Workaround: When inserting a stacking module, ensure the system is powered down first.

PR# 77977

Severity: S3

Synopsis: A "write memory" operation executed immediately after reload of a stack unit may fail.

Release Notes: A "write memory" operation executed immediately after reload of a stack unit may fail.

Workaround: Wait for the stack-unit reload to complete for executing this operation.

PR# 77995

Severity: S4

Synopsis: A stack upgrade operation as initiated via the "upgrade system stack-unit" command cannot be cancelled once initiated.

Release Notes: A stack upgrade operation as initiated via the "upgrade system stack-unit" command cannot be cancelled once initiated.

Workaround: Take care in executing the "upgrade" command.

PR# 78135

Severity: S2

Synopsis: Configurations related to 10GE module may be lost upon stack reload if the stack-unit rejoins after the master unit comes online.

Release Notes: 10-GE interface configurations may be lost upon stack reload if the stack-unit rejoins after the master unit comes online. This issue results from the S-Series not having a logical module concept specifically for 10-GE interfaces. Other interfaces are not affected.

Workaround: None. Re-apply the 10-GE configuration after a stack reload if the stack-unit with the 10-GE module comes up after the master unit.

PR# 79858

Severity: S2

Synopsis: In a stack of 8 S-Series switches stacking links may flap when "show tech-support | save" command is issued.

Release Notes: In a stack of 8 S-Series switches stacking links may flap when "show tech-support | save" command is issued, to save the output of 'show tech' to a file.

Workaround: None. Avoid using this command with large number of stack units

PR# 80916

Severity:	S2
Synopsis:	In rare cases, after rebooting an S-Series stack, the standby stack-unit status is not fully processed by the system.
Release Notes:	In rare cases, after rebooting an S-Series stack, the standby stack-unit status is not fully processed by the system. While the "show system brief" command indicates that the standby unit is online, the "show redundancy" command will display that the stack-unit state of the standby is "Booting" and the software version is "unknown".
Workaround:	When this condition is occurring, no functionality should be impacted.

PR# 81007

Severity:	S1
Synopsis:	Very rarely SWP timeout between DiffServMgr and DiffServAgent could be seen when renumbering stack units in S-Series.
Release Notes:	Very rarely SWP timeout between DiffServMgr and DiffServAgent could be seen when renumbering stack units in S-Series. The failure will cause the stack to reboot automatically.
Workaround:	None.

DHCP (Open)

PR# 81259

Severity:	S2
Synopsis:	After failover, Binding entry for DHCP snooping may not get removed for DHCP Release messages.
Release Notes:	After failover, DHCP snooping binding entry may not get removed for DHCP Release messages from DHCP client.
Workaround:	After failover, remove any port from snooped vlan and add it again or reload the Chassis.

PR# 81274

Severity:	S2
Synopsis:	Snooping binding table will be lost after failover or reload if dhcpBinding file is not available in flash.
Release Notes:	After failover, DHCP snooping binding table will be populated from dhcpBinding file in flash. Snooping table will be lost after failover or reload, if dhcpBinding file is not available in flash on both Primary and Standby RPM.
Workaround:	Configuring a lower value on write-delay time can minimize the risk as it will create the dhcpBinding file sooner.

VLAN Stack (Open)

PR# 78327

Severity:	S4
Synopsis:	The "M" flag in the "show vlan'" command output is not defined at top with all other flags.
Release Notes:	The "M" flag in the "show vlan'" command output is not defined at top with all other flags. The "M" refers to interfaces which are members in a VLAN-stack.
Workaround:	None. This PR requests that the flag description be added.

Technical Support

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.

Accessing iSupport Services

The URL for iSupport is www.force10networks.com/support/. To access iSupport services you must have a user identification (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 user identification and password by E-Mail.
3. To access iSupport services, click the **Log in** link, and enter your user identification and password.

Contacting the Technical Assistance Center

How to Contact Force10 TAC	Log in to iSupport at www.force10networks.com/support/, and select the **Service Request** tab.
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 • Software version number • Symptom description • Screen shots illustrating the symptom, including any error messages. These can include: •Output from the **show tech** command or the **show tech linecard** command. •Output from the **show trace** command or the **show trace linecard** command. •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 Web: www.force10networks.com/support/ Telephone: US and Canada: 866.965.5800 International: 408.965.5800

Requesting a Hardware Replacement

To request replacement hardware, follow these steps:

Step	Task
1.	Determine the part number and serial number of the component. To list the numbers for all components installed in the chassis, use the **show inventory** command.
➡	**Note:** The serial number for fan trays and AC power supplies might not appear in the hardware inventory listing. Check the failed component for the attached serial number label. Quickly reinsert the fan tray back into the chassis once you have noted the serial number.

Step	Task
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 52). • Contacting Force10 directly by E-mail or by phone (see Contacting the Technical Assistance Center on page 52). 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: • the **show tech** command output • the **show trace** and **show trace hardware** command output • for line card issues, the **show trace hardware linecard** command output • console captures showing any error messages • console captures showing the troubleshooting steps taken • saved messages to a syslog server, if one is used • The support representative will validate your request and issue an RMA number for the return of the component.
3.	Pack the component for shipment, as described in the hardware guide for your system. Label the package with the component RMA number.

MIBS

Force10 MIBs are currently under the **Force10 MIBs** subhead on the **Documentation** page of iSupport:

https://www.force10networks.com/csportal20/KnowledgeBase/Documentation.aspx

You also can obtain a list of selected MIBs and their OIDs at the following URL:

https://www.force10networks.com/csportal20/MIBs/MIB_OIDs.aspx

Some pages of iSupport require a login. To request an iSupport account, go to:

https://www.force10networks.com/CSPortal20/Support/AccountRequest.aspx

If you have forgotten or lost your account information, send an e-mail to TAC to ask that your password by reset.